AP-Journal

GUI™

The Database Modification Component of iSecurity

iSecurity GUI 4 User Manual

RAZ-LEE™
The iSeries Security Experts

Updated: 04/19/2010

Copyright Notice

© Copyright Raz-Lee Security Inc. All rights reserved.

This document is provided by Raz-Lee Security for information purposes only.

Raz-Lee Security© is a registered trademark of Raz-Lee Security Inc. Action, System Control, User Management, Assessment, Firewall, FileScope, Screen, Password, Audit, Capture, View, Visualizer, Anti-Virus, AP-Journal © are trademarks of Raz-Lee Security Inc. Other brand and product names are trademarks or registered trademarks of the respective holders. Microsoft Windows© is a registered trademark of the Microsoft Corporation. Adobe Acrobat© is a registered trademark of Adobe Systems Incorporated. Information in this document is subject to change without any prior notice.

The software described in this document is provided under Raz-Lee's license agreement.

This document may be used only in accordance with the terms of the license agreement. The software may be used only with accordance with the license agreement purchased by the user. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, without written permission given by Raz-Lee Security Inc.

Visit our web site at www.razlee.com.

Record your product authorization code here.

Computer Model	
Serial Number	
Authorization Code	

About This Manual

Who Should Read This Book

This user guide is intended for all System i system administrators and in particular for security administrators responsible for the implementation and management of security on System i systems.

Terminology

This manual attempts to adhere to standard IBM iSeries (System i) terminology and conventions whenever possible. However, deviations from IBM standards are employed in certain circumstances in order to enhance clarity or when standard IBM terminology conflicts with generally accepted industry conventions.

Documentation Overview

Raz-Lee takes customer satisfaction seriously. Therefore, our products are designed for ease of use. The documentation package includes a variety of materials to get you up to speed with this software quickly and effectively.

Printed Materials

This user guide is the only printed documentation necessary for understanding this product. It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 4.0 or higher. Acrobat Reader is included on the product CD-ROM.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

On-Line Help

PC based on-line help is also available in JavaHelp format. Click the Help button from your Firewall menubar.

Typography Conventions

This document is intended to be printed by the end user and viewed on-line using a variety of different PC platforms. Accordingly, it was written using standard Windows TrueType fonts that are installed on virtually all systems. You do not need to install any special fonts in order to view or print this document.

- Body text appears in 10-point Times New Roman.
- Menu options, field names, and function key names appear in **Arial Bold**.
- OS/400 commands, system values, data strings, etc. appear in ***Bold Italic.***
- Key combinations are separated by a dash, for example: **Shift-Tab**.
- Referrals to chapters or procedures appear in *Times New Roman Italic*.

Table of Contents

Copyright Notice i

About This Manual ii
Who Should Read This Book ii
Terminology ii
Documentation Overview ii
Printed Materials ..... *ii*
On-Line Help ..... *ii*
Typography Conventions ii

Chapter 1: Introducing iSecurity 4
What is iSecurity? 4
Why You Need iSecurity 4
How iSecurity Works 4
Top-Down Security Design *4*
iSecurity Rules and the Best Fit Algorithm *5*
FYI Simulation Mode *6*
Emergency Override *6*
Rule Wizards *6*
Activity Log *6*
Business Intelligence - Visualizer *6*
System Requirements 7
iSecurity 8
Assessment *8*
Firewall *8*
Audit *8*
Action *8*
Anti-Virus *9*
View *9*
Capture *9*
Screen *9*
Password *9*
AP-Journal *9*

Chapter 2: Getting Started 12
Create a New Account 12
Running iSecurity GUI in SSL mode 14
SSL Settings *16*
Security 17
Secure Storage *17*
Delete Secure Storage *17*
Account Information Properties 18

Connection timeout *20*
Item *21*
Deleting an Account 23
Account Sessions 24
Creating a New Session 25
Disconnecting a Session *28*
Session Properties *29*
Item *30*
Session *31*
Reset Window 33
Show View 34
Application Password 35
Screens and Editors 35
Editors *36*
Nodes with filter 37
Show entry content *39*
Update 40
Check for updates in one click *40*
Automatic and Scheduled Updates *41*
iSecurity Archived Update Site *42*
Reporting problems in iSecurity GUI 43
Log Preferences window *43*
Help 45
Define Default Settings *45*
Editors 46
Last Modified Editor *49*
Editor Display *50*
Print format *51*
Open editor display *52*
Editor Filter *53*
Rule Wizards 55
Preferences 57

Chapter 3: AP-Journal 62
Workflow 62
Application Definitions 62
Adding Application *62*
Add File to the Application *70*
Set File Definitions *72*
Enable Application 77
Status 77
Add a New Action 78
Edit Actions *82*
Application Outputs 82

Chapter 3: Introducing Business Intelligence Visualizer 92

Overview 92
Key Features and Benefits 92
Installing Business Intelligence - Visualizer 92

Chapter 3: Working with Business Intelligance 94
Working with Business Intelligence 94
Starting Business Intelligence 94
The Business Intelligence Interface 96
Generating Graphic Reports 99
Purge history files of Visualizer by SQL 104

Appendix: License Agreement ii
Preamble ii
GNU LESSER GENERAL PUBLIC LICENSE iii

1 Introducing iSecurity

Chapter 1: Introducing iSecurity

What is iSecurity?

iSecurity is a comprehensive network security solution that completely secures your System i against all known external threats, and also controls what users are allowed to do **after** access is granted. **iSecurity** is a robust, cost-effective, security solution.

iSecurity is by far the most intuitive and easy-to-use security software product on the market today. Its top-down functional design and intuitive logic create a work environment that even novices can master in minutes. **iSecurity** features a user-friendly, Java-based GUI and an System i Navigator (OpsNav) plug-in.

Why You Need iSecurity

Once upon a time, the System i was used almost exclusively in a closed environment, with host systems connected to remote data terminals via proprietary technologies. Within this closed environment, the security features of the OS/400 operating system provided the strongest data and system security in the world. User profiles, menus, and object level security provided all the tools necessary to control what users were allowed to see and do.

In today's world of enterprise networks, PCs, distributed databases, the Internet and web technologies, closed computing environments are all but extinct. Technological advances compelled IBM to open up the System i and its OS/400 operating system to the rest of the world. This new "openness" brought with it many of the security risks inherent in distributed environments.

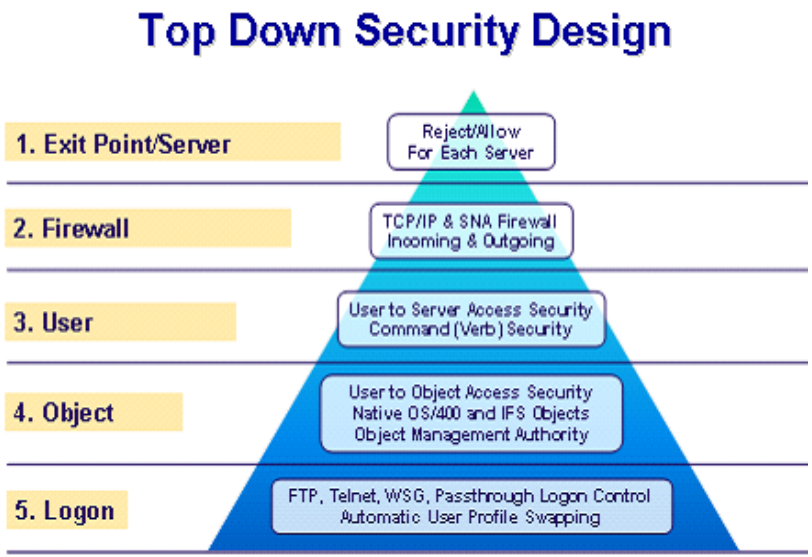
The simple fact is that users accessing the System i and its databases externally can easily bypass native OS/400 security. System administrators need to equip themselves with a new generation of security tools to combat these evolving threats. **iSecurity** is just such a tool. It enhances native OS/400 by controlling access via all known external sources and controlling precisely what users are permitted to do once access is granted.

How iSecurity Works

Top-Down Security Design

Top-down security design means that the process of designing and applying security rules follows the most efficient and logical path possible. In other words, this means you have to design far fewer rules in order to achieve maximum security and your System i needs to process apply rules to far fewer transactions than many similar products. You save planning and maintenance time as well as valuable system resources.

Top-down security designs a simple hierarchy of rule types. When a higher level rule type fully meets your security requirements, you do not need to define any more rules for that situation. The following drawing illustrates this concept.



iSecurity Top-Down Security Design

System i security is based on five basic levels:

- Server/Exit Point Security
- TCP/IP Address Firewall Security
- User-to-Service Security
- Object Security
- Logon Security (provides additional security features once access has been granted)

Simply put, whenever a higher, less specific rule will suffice, you do not need any more specific rules. For example, if you do not need to use FTP, you simply reject all transactions at the FTP Server/Exit Point level. You do not need to define any rules that limit FTP access via specific IP addresses, by specific users, or to specific objects.

iSecurity Rules and the Best Fit Algorithm

iSecurity is a rules-based security product. You create a wide variety of rules to cover many different situations and to counter different kinds of threats. Some rules will likely apply globally to all or most activity types while others will be designed to cover very specific situations.

You can enable FYI Simulation mode globally for all activity regardless of server or user. You can also enable FYI individually for specific function servers as a parameter in server security rules. In this manner, you can test security rules for specific servers without affecting rules that apply to other servers.

FYI Simulation Mode

FYI Simulation mode allows you to simulate the application of security rules without physically rejecting any activity. All "rejected" transactions are recorded in the Activity log as such but the activity is allowed to proceed without interruption. This feature allows you to test your rules under actual working conditions without adversely affecting user success.

FYI Simulation mode may be enabled globally for all activity or enabled for individual function servers. In this manner, you can test security rules for specific servers without affecting rules that apply to other servers.

Emergency Override

The Emergency Override feature allows you to override all existing security rules temporarily by allowing or rejecting all activity. feature is useful in order to respond quickly to emergencies such as critical transactions being rejected due to problems with **iSecurity** security rules or a sudden security breach.

Rule Wizards

The unique Rule Wizards feature makes security rule definition a snap, even for non-technical system administrators. This user-friendly feature allows you to view historical activity together with the security rule currently in effect on a single screen. You can even modify the existing rule or define a new rule without leaving the wizard! The Rule Wizards are an invaluable tool for defining the initial set of rules after installing **iSecurity** for the first time.

Activity Log

The Activity Log provides complete details of every transaction captured by a security rule. You have full control over which activities are included in the Activity Log and under which conditions.

Highly-defined filter criteria allow you to select only those records that you need to examine by using Boolean operators and the ability to combine complex logical conditions. You have full flexibility to specify the sort order according to multiple fields.

Business Intelligence - Visualizer

Visualizer is an advanced data warehouse solution for graphically displaying security data. It allows IT managers to analyze security-related system activity quickly and easily using a

stunning graphical interface. **Visualizer** eliminates the need for time-consuming log-scanning and tracking activities that tie up system resources and increase operating costs.

System Requirements

- PC workstation - (due to the use of Java 6)
  - Windows XP Professional (SP1)
  - Windows XP Home
  - Windows 2000 Professional (SP3+)
  - Windows Server 2003, Web Edition
  - Windows Server 2003, Standard Edition
  - Windows Vista

- Operating system - GUI connects to V5R1 and higher of OS400
- Minimum RAM - at least 128M
- TCP/IP communication to the iSeries or AS/400.
  - STRTCPSVR SERVER(*DDM) to start the TCP/IP server (with *DDM specified for the Server parameter).
  - Host servers should be started on the server. (STRHOSTSVR SERVER(*ALL) from the as400 command prompt).
  - QUSER user profile enabled and has a valid password.
  - Disk Space Required - currently, at least 160M but it is going to grow (I don't have an estimation yet)

iSecurity

Raz-Lee's **iSecurity** is an integrated, state-of-the-art, security solution for all System i systems, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security. Other **iSecurity** products include:

Assessment

Assessment checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.

Firewall

Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. **Firewall** manages user profile status, secures entry via pre-defined entry points, and profiles activity by time. Its Best Fit algorithm determines the validity of any security-related action, hence significantly decreasing system burden while not compromising security.

Audit

Audit is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit can also trigger customized responses to security threats by means of the integrated script processor contained in **Action**.

Action

Action automatically intercepts and responds to security breaches, system activity events, QHST contents, and other message queues. Inquiring messages can be automatically answered. Alerts are sent by e-mail, SMS, pagers, or the message queues. Command scripts with replacement variables perform customized corrective actions, such as terminating a user session or disabling a user profile.

Anti-Virus

Anti-Virus provides solid virus protection that prevents your System i from becoming an infection source. **Anti-Virus** automatically scans and examines all incoming IFS files, validating and checking them as they are enrolled or modified. Anti-Virus authenticates them, and finally quarantines or erases infected files.

View

View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, etc. Restricted users see asterisks or zeros instead of real values. **View** requires no change in existing applications. It works for both SQL and traditional I/O.

Capture

Capture silently captures and documents user screens for tracking and monitoring, without any effects on system performance. It also preserves job logs for subsequent review. capture can run in playback mode and can be used to search within texts.

Screen

Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific time-out capabilities.

Password

Password provides a first-tier wall of defense for users by ensuring that user passwords cannot be easily cracked and guessed.

AP-Journal

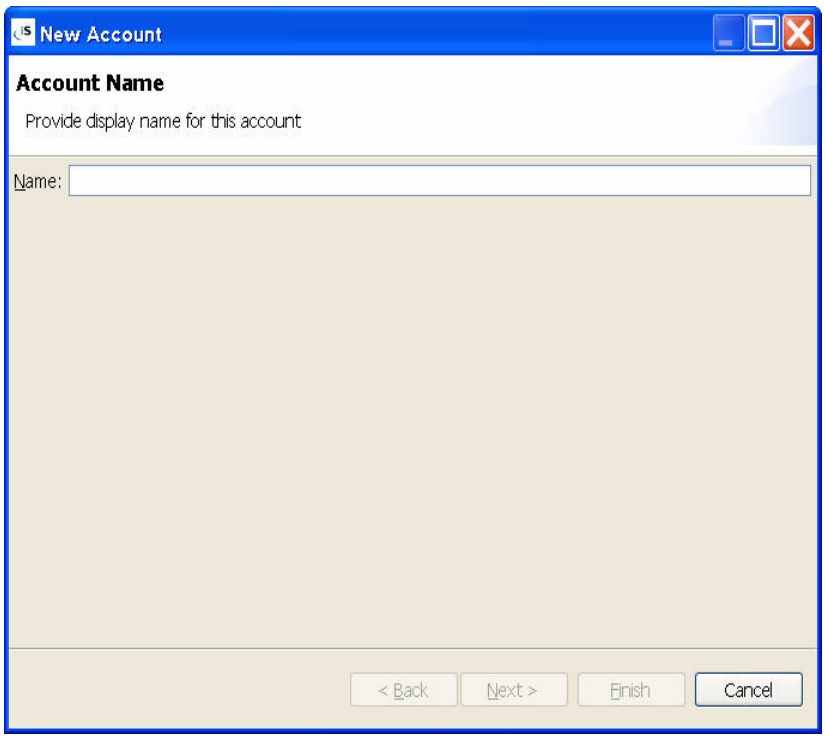
AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal.

2 Getting Started

Chapter 2: Getting Started

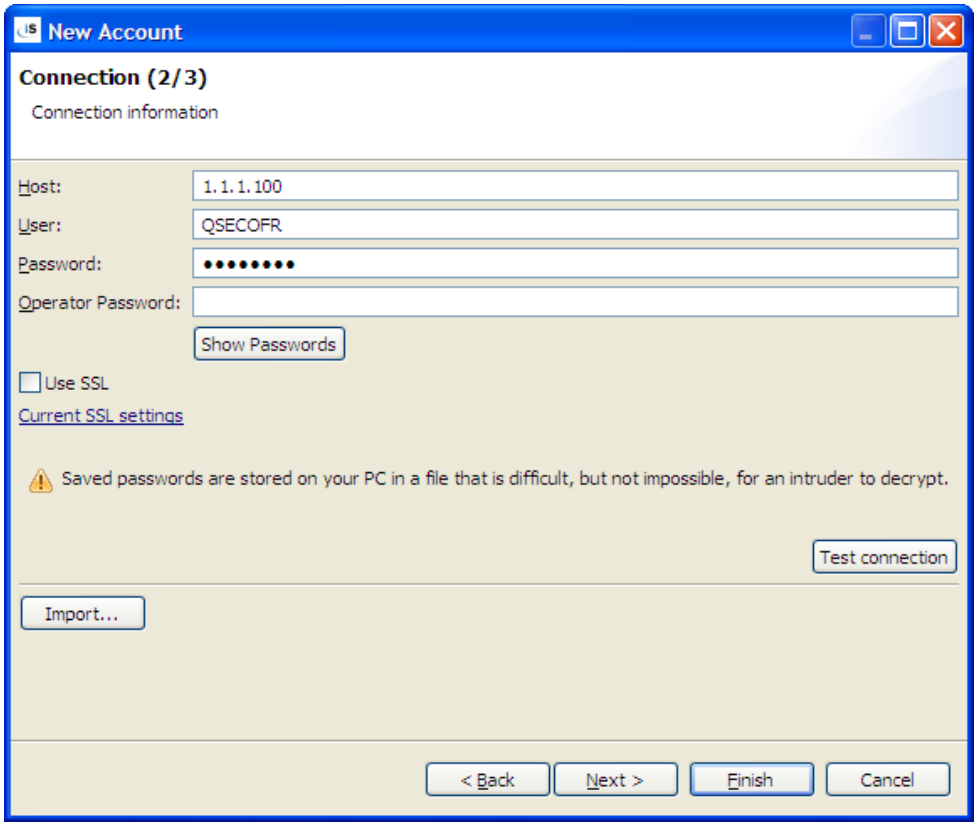
Create a New Account

1. Click the **iSecurity** symbol on your desktop.
2. Right-click in the iSecurity navigator view
3. Select **New Account...,** the **Account Name** screen appears. Type account name and click **Next**



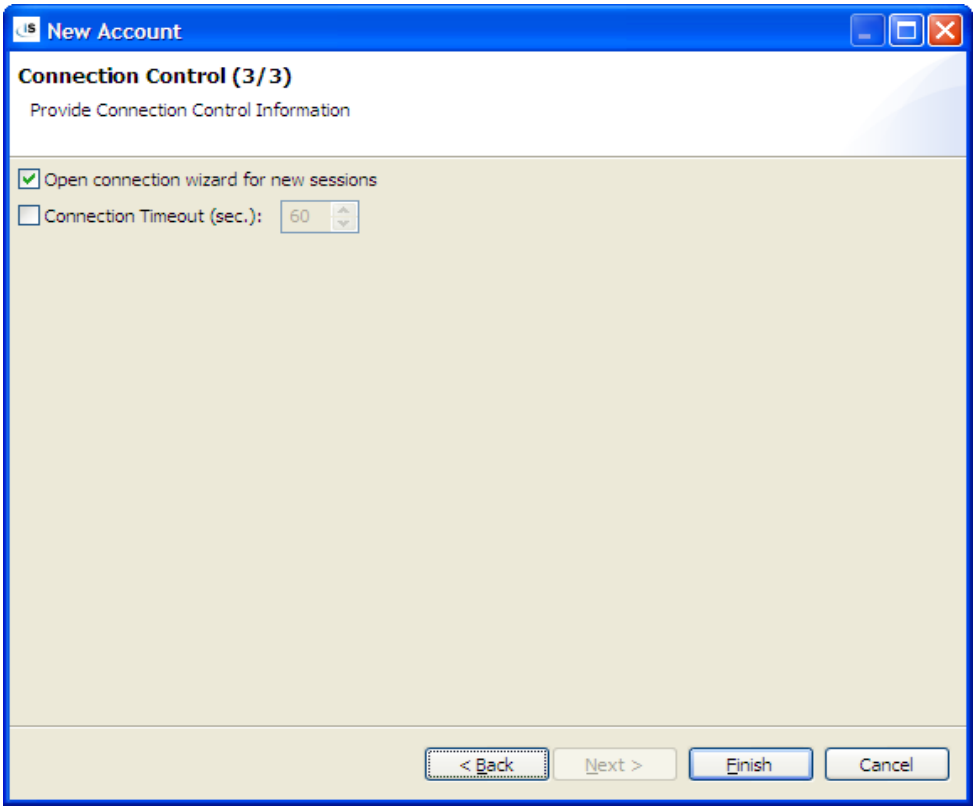
New Account

4. In the **Connection** screen, enter **Host**, **User**, and **Password** in the correct fields, and click **Finish** or **Next**



New Account - Connection

5. When clicking **Next,** the **Connection Control** screen appears. Check the **Open Connection Wizard** if you whish the application to prompted for new sessions. This is just a conveniences issue that suits those cases where all required information for making a connection is supplied.
6. Check the **Connection Timeout** and type after how man seconds to stop the attempt to connect.



Connection Control

NOTE: *The only required field for an account is a name. The account stores user's data on the disc in a file that is difficult but not impossible for an intruder to read, so care should be taken here.*

Running iSecurity GUI in SSL mode

Encrypt the link between any sensitive file and the GUI interface using Eclipse SSL system.

1. Open a web browser to your Power i system (usually, port 2001 is used). Click on "Digital Certificate manager", On the left, click on "Install Local CA Certificate on Your PC", click on "Copy and paste certificate". Cut and paste the certificate into notepad, save the file with a name such as "ca.txt" to iSecurity installation location (c:\programfiles\isecurity by default).
2. On your PC open the command prompt and change directory to iSecurity installation location (c:\program files\isecurity by default)

3. From that location use the Java tool keytool to import the certificate into a trust list. Issue the command: "jre\bin\keytool -import -v -trustcacerts -alias <aliasName> -file ca.txt -keystore trustlist". (alias is just optional) This will create a file called "trustlist" and during the command it will prompt you to establish a password for this file.
4. This step can be performed either from command line or from within the GUI itself.

   - Command line: From the command prompt from within the iSecurity installation location issue this command: isecurity.exe -vmargs -Djavax.net.ssl.trustStore=trustlist-Djavax.net.ssl.trustStorePassword=pwd

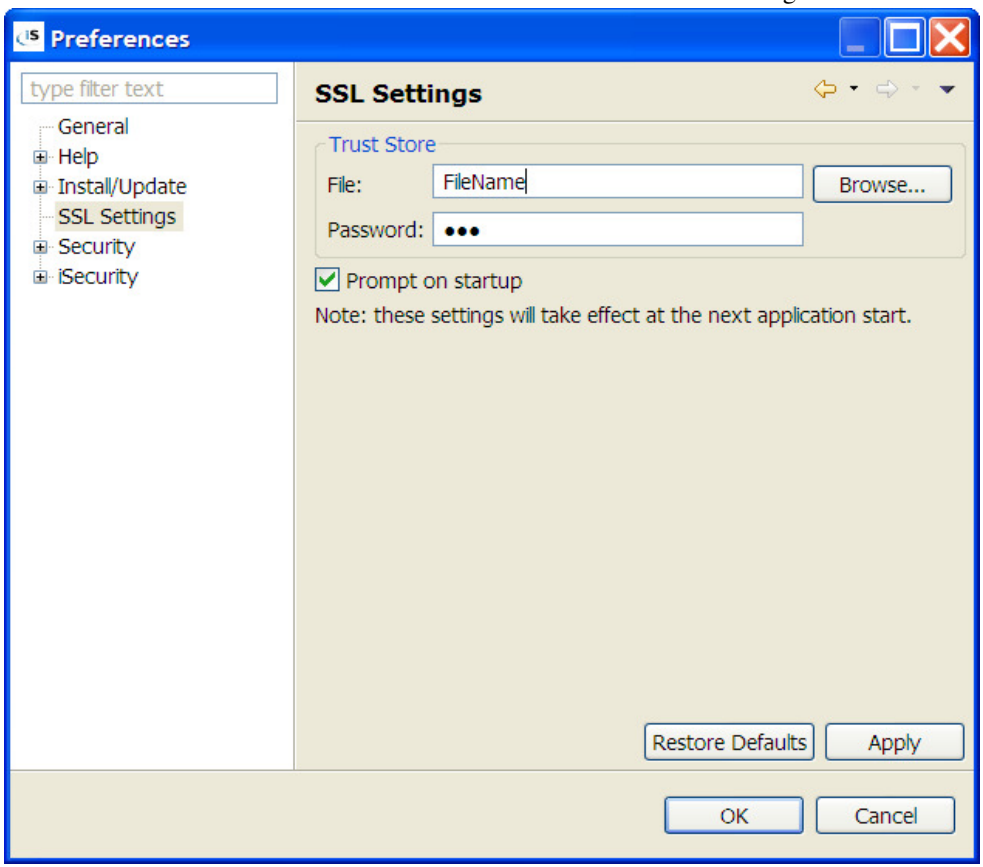
Replace trustlist and password with your own (these are the parameters used in step 3)

The trustlist parameter is the absolute path to the file itself including file name (c:\....\trustlist) but if this file resides on iSecurity installation location, there is no need to type the path.

- GUI

SSL Settings

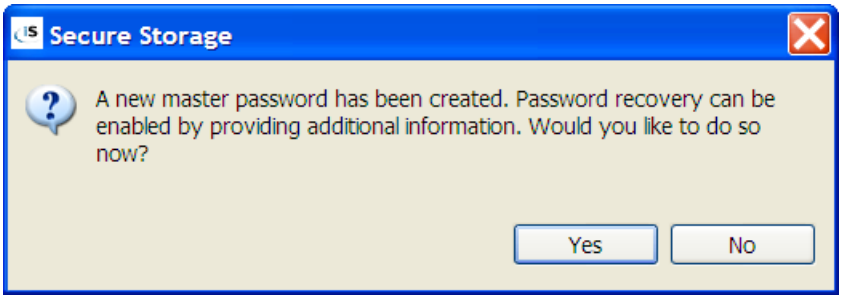
1. From the menu-bar select Window -> Preferences -> SSL Settings



Preferences - SSL Settings

2. To keep the SSL connection in high security level, check the **Prompt on Startup** check box and leave the **File** and **Password** fields empty. If you don't want the prompt, type the file name and access password and leave the check box empty.
3. Click **Apply** or **OK**. These settings take affect only once at application start

Windows users: a Master Password will automatically be created according to the Windows logon user/password in use


Secure Storage
A new master password has been created. Password recovery can be enabled by providing additional information. Would you like to do so now?
Yes
No

Secure Storage

Linux users: **create a Master Password** dialog box will be prompt

4. The next time the iSecurity GUI will start, the SSL Settings dialog box will prompt asking for the secured file name and access password.

Security

Secure Storage

The secure storage is located at: **Window -> Preferences -> Security ->Secure Storage** and saves data in an encrypted form. On some operating systems, it uses your operating system account information to provide a single sign-on experience.

The secure storage itself does not contain encryption code. It uses algorithms supplied by the Java virtual machine and/or the operating system.

The secure storage also contains the Windows account information in an encrypted form, which means that without the Windows account password there is no access to the Power i sensitive data. The information in the secure storage is encrypted in the strongest way that even if the encrypted information file is stolen, there is no way to crack it.

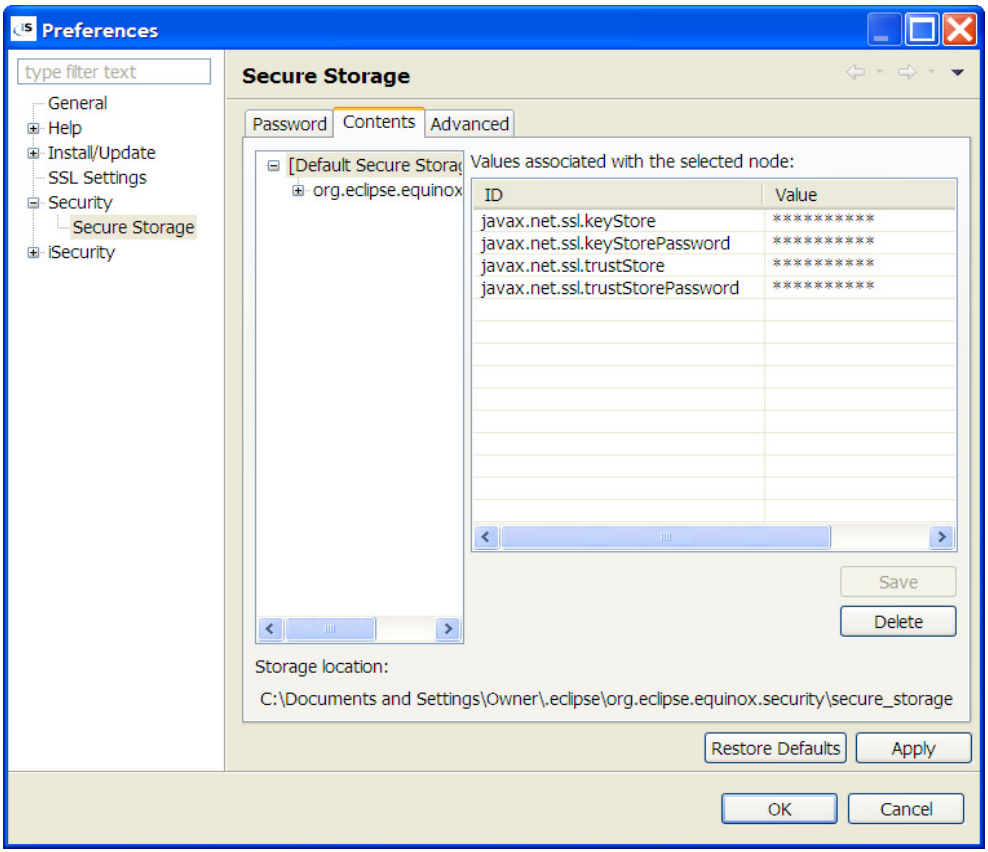
NOTE: *Read more about Secure Storage in iSecurity Help*

Delete Secure Storage

Delete the Secure Storage information follow this procedure:

1. From the toolbar go to **Window -> Preferences -> Security ->Secure Storage**
2. Select the **Contents** tab

3. Click to select the **Default Secure Storage**



Secure Storage

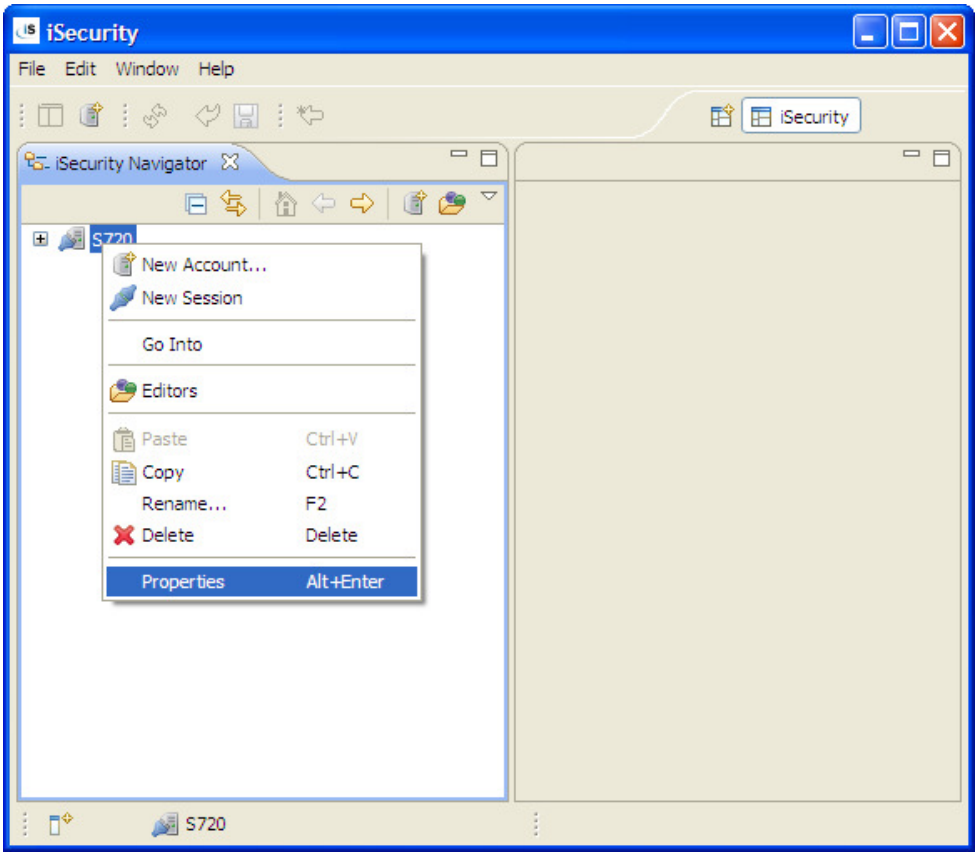
4. Click **Delete** to clean the storage

NOTE: *learn more about Secure Storage from the help content*

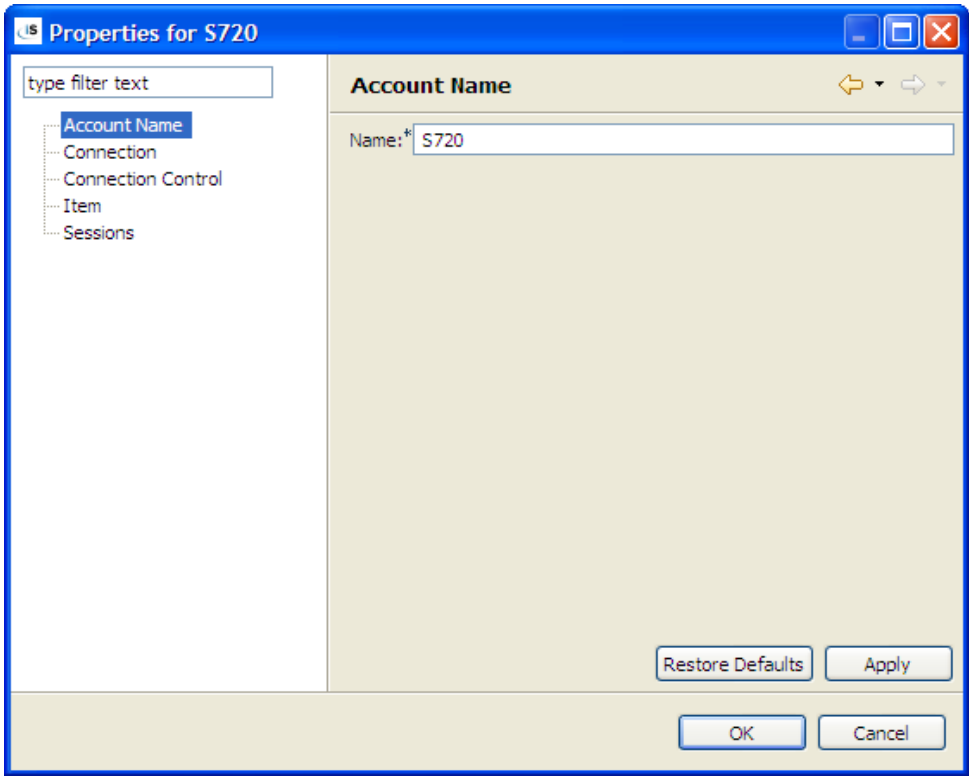
Account Information Properties

Once an account is created it is added to iSecurity navigator.

An account can be modified by right clicking on it and selecting **Properties**



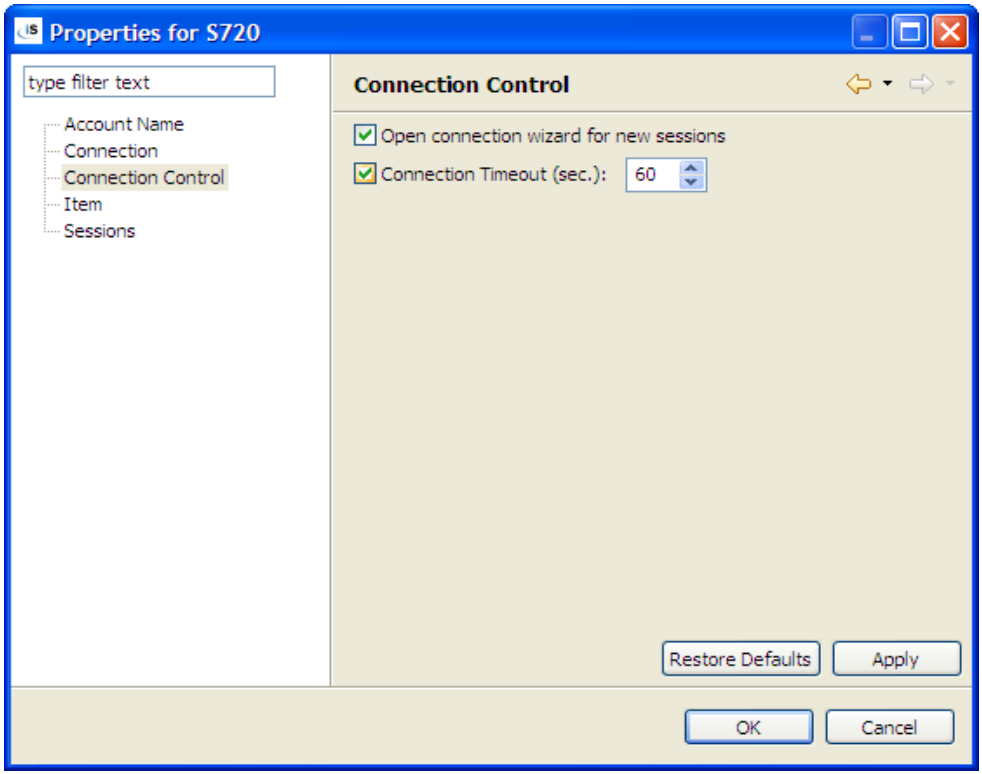
Account Properties



Account Properties

Connection timeout

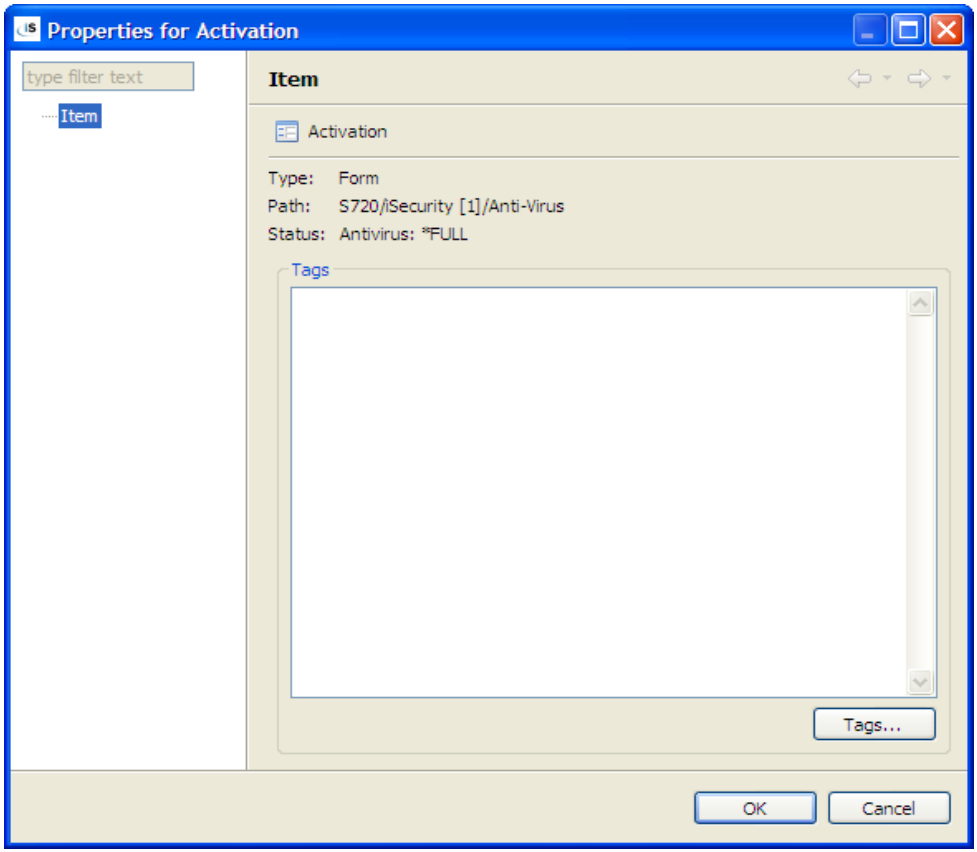
GUI will stop the attempt to connect after the specified time defined in **Connection Control**



Connection Control

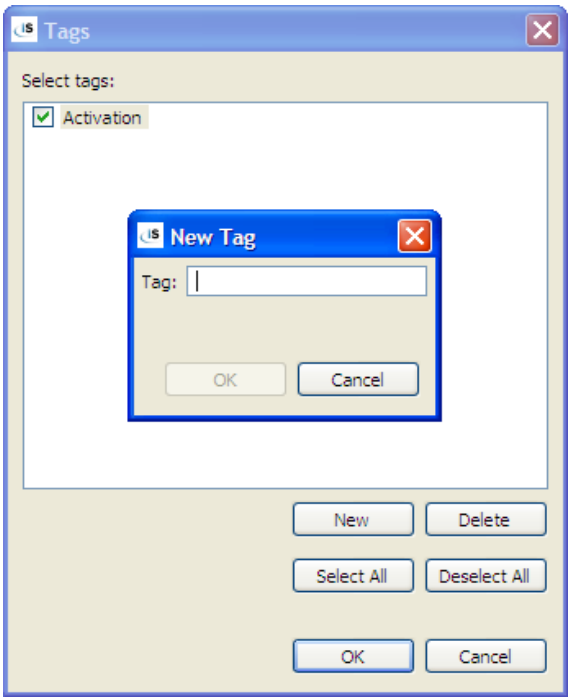
Item

Display node authorization and tag it for easier search of the specific item in the GUI application.



Properties Item

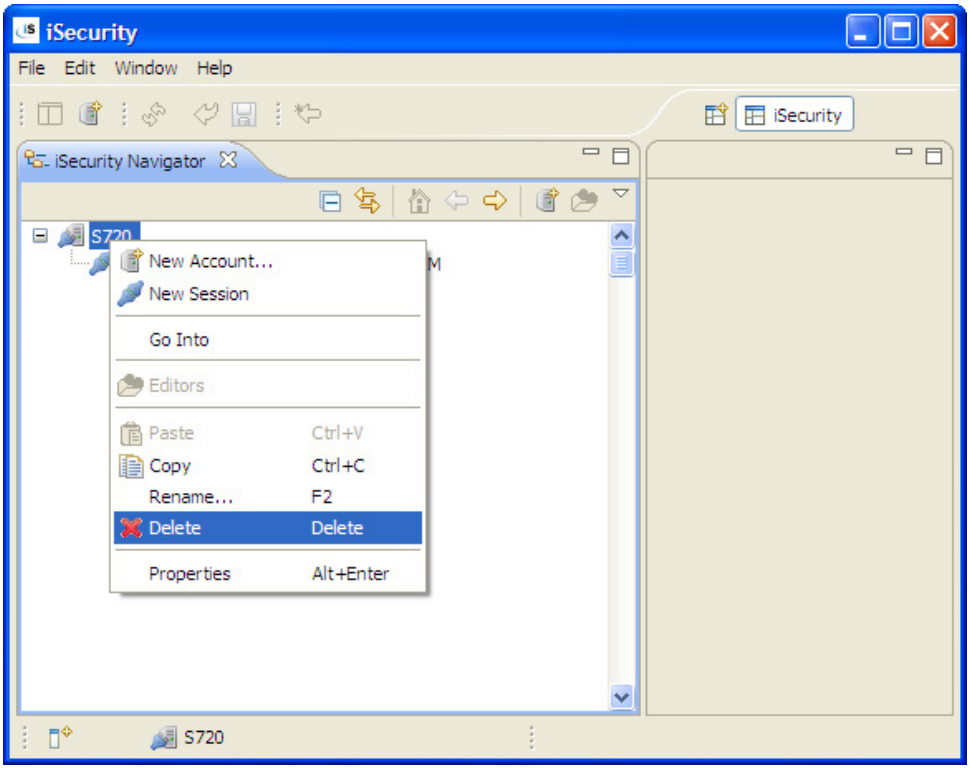
Add a new tag or assign an existing one



Tag

Deleting an Account

Account can be deleted by right clicking on it and selecting **Delete**



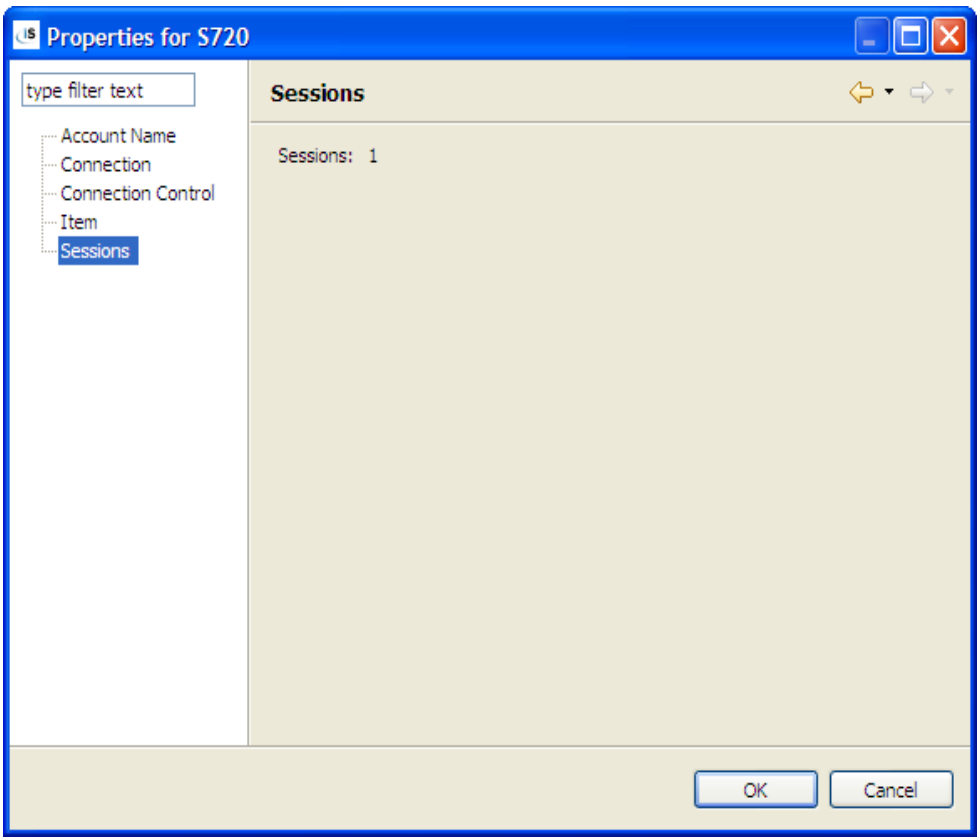
Delete Account

Deleting account will disconnect all sessions under this account.

NOTE: *If a session has an unsaved data the user will receive a warning asking him to confirm the action.*

Account Sessions

Select Sessions to view how many sessions are open for this account

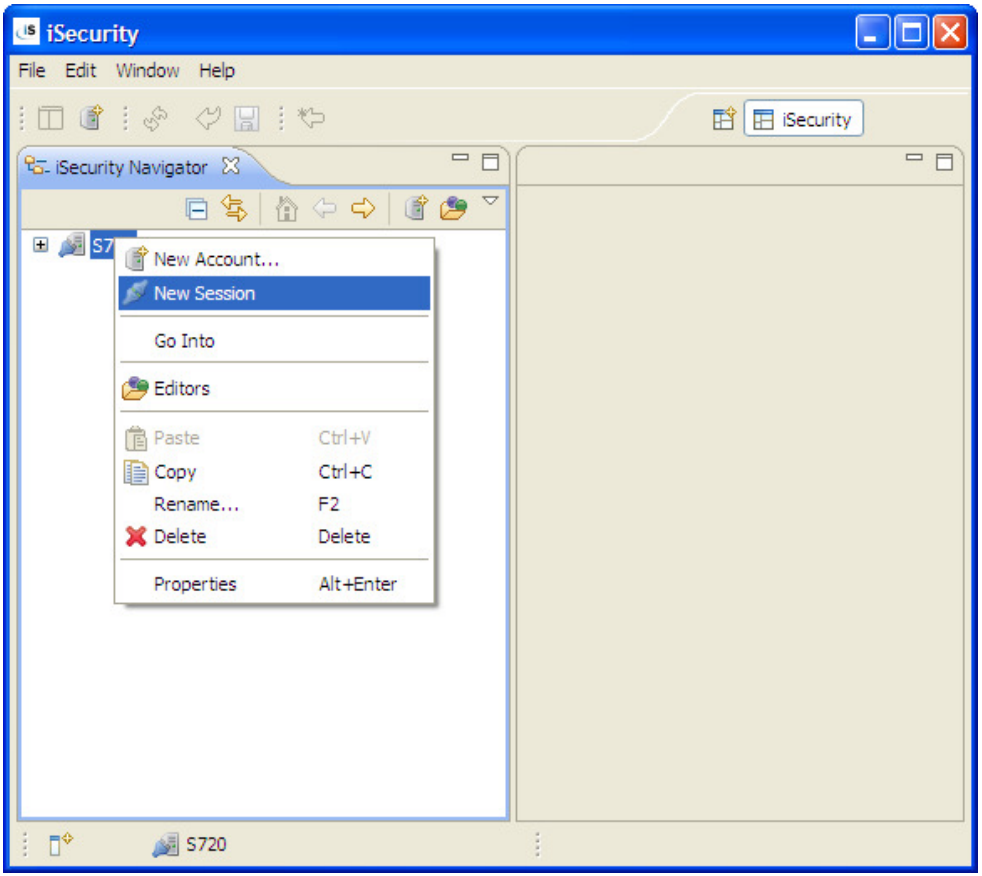


Sessions

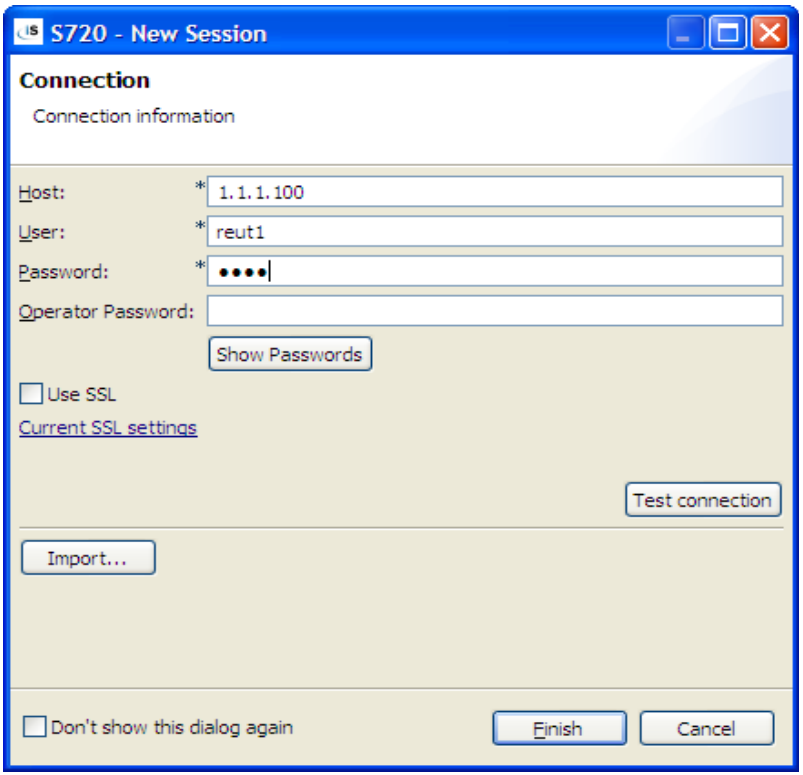
Creating a New Session

There are three options to create a new session based on the account's data:

- Right click the account and select **New Session**
- Double click the account (if it hasn't got sessions)
- Click on the node's handle (if it hasn't got sessions)


iSecurity
File Edit Window Help
iSecurity
iSecurity Navigator
New Account...
New Session
Go Into
Editors
Paste Ctrl+V
Copy Ctrl+C
Rename... F2
Delete Delete
Properties Alt+Enter
S720

New Session



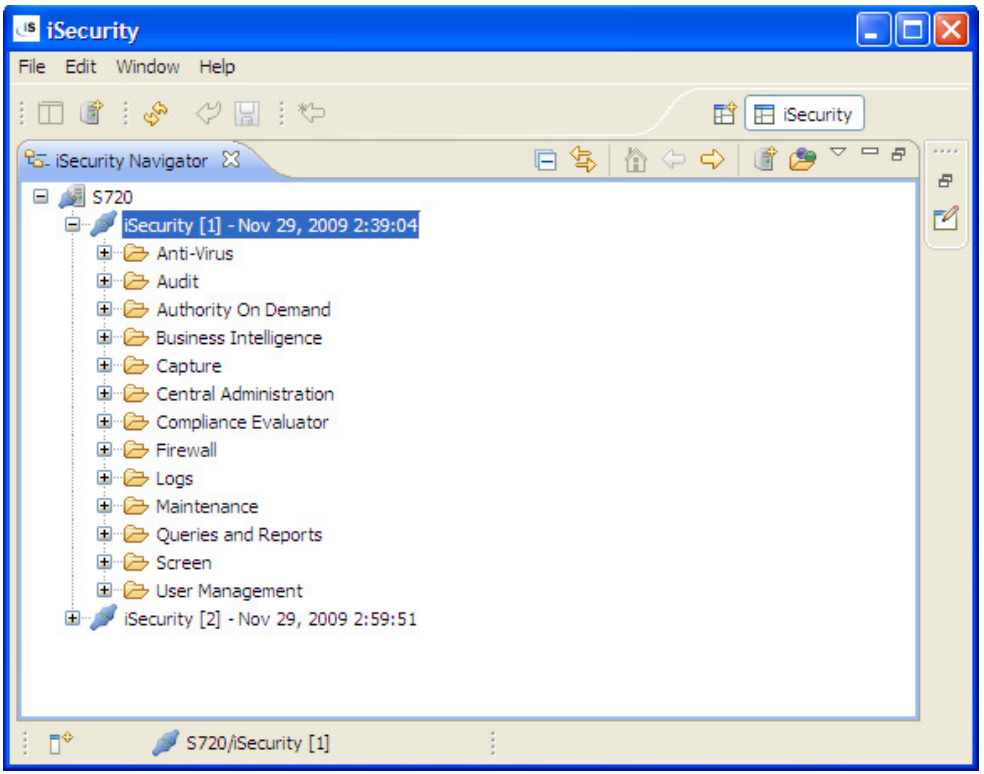
New Session Connection

- Click **Import** to import a pre saved connection data upon creation of an account.
- Check the "**Don't show this dialog box again**" to prevent prompting for new sessions of this account.

NOTE: *Data supply in this step has no persistence on disc*

Click **Finish** to connect to supplied host. Connection process runs in the background enabling the user to continue working.

A new session node added to the account along with the nodes of the application

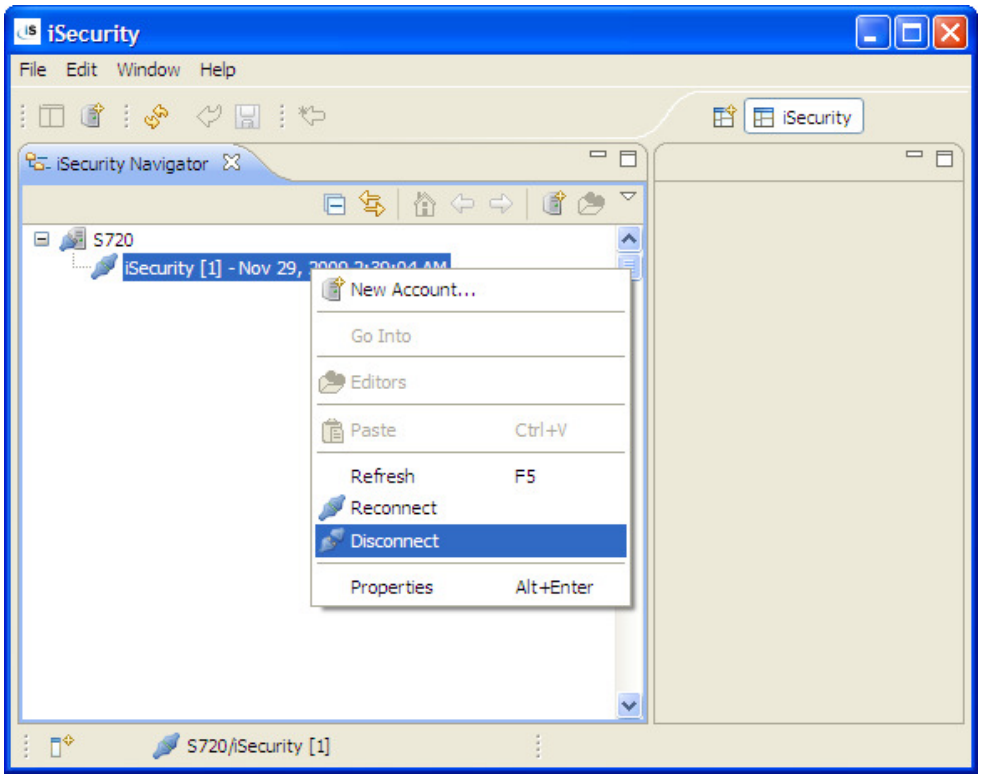


New Session Added

Multiple sessions can be added based on the same account or different under the same account. Multiple accounts can also be created.

Disconnecting a Session

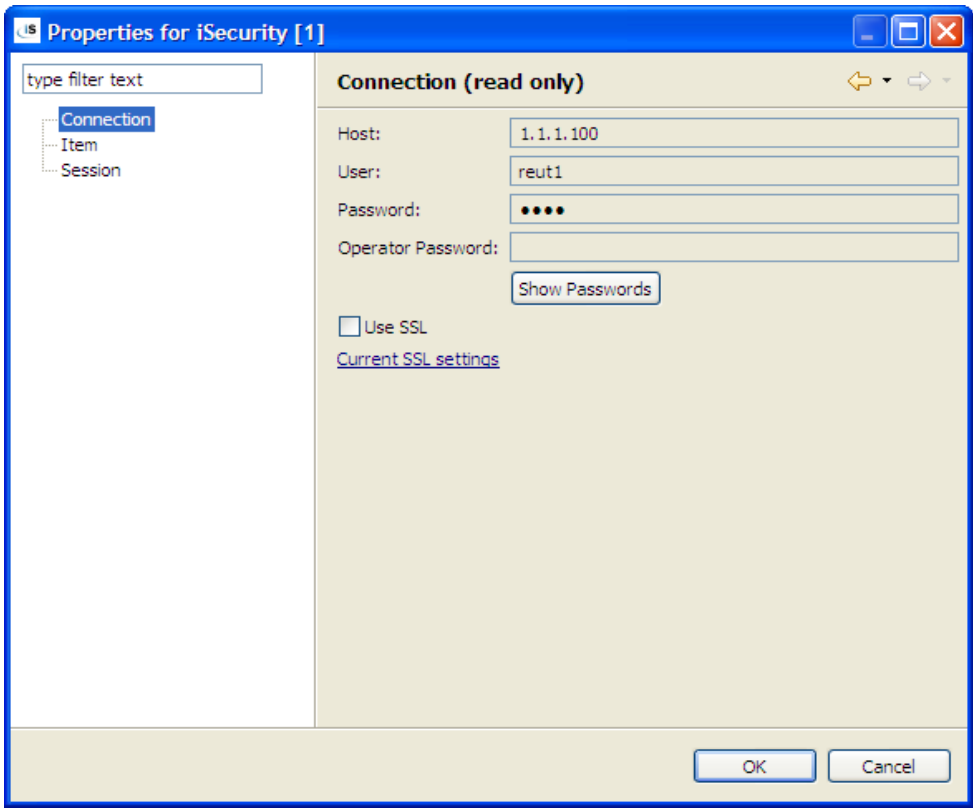
To disconnect from a session, right click on a session title or on multiple sessions and select **Disconnect**



Disconnect Session

Session Properties

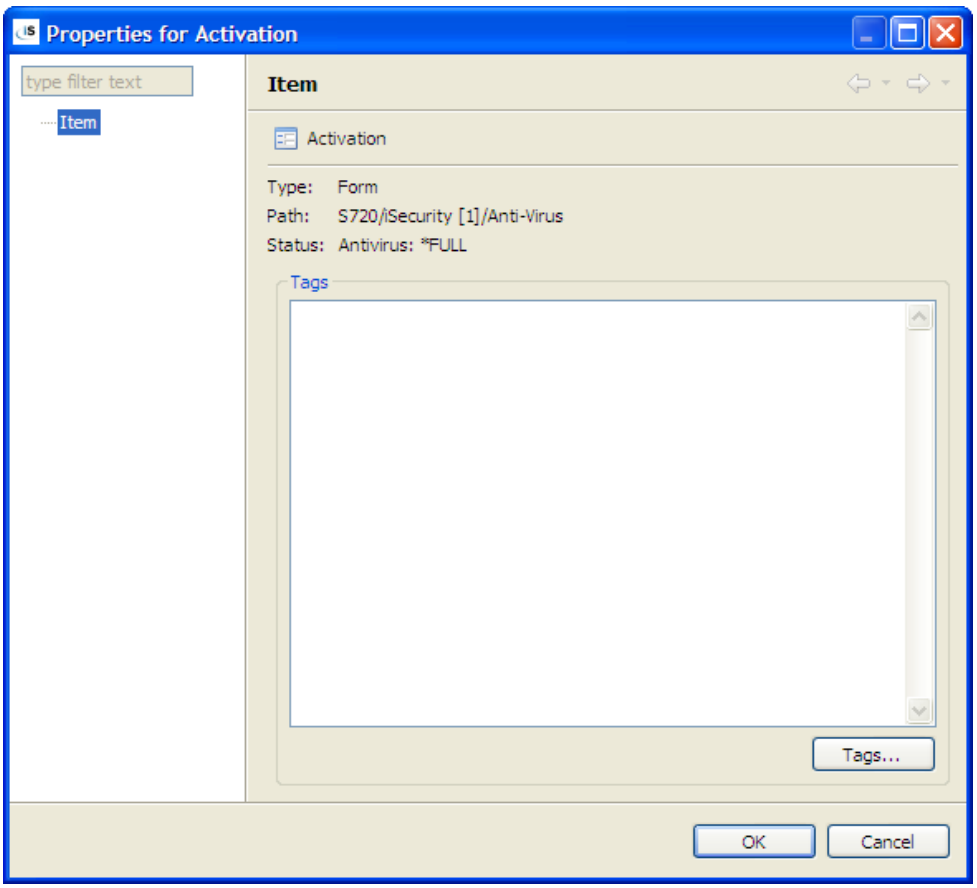
Session properties are read only information, the connection can not be modified.



Session Properties - Connection

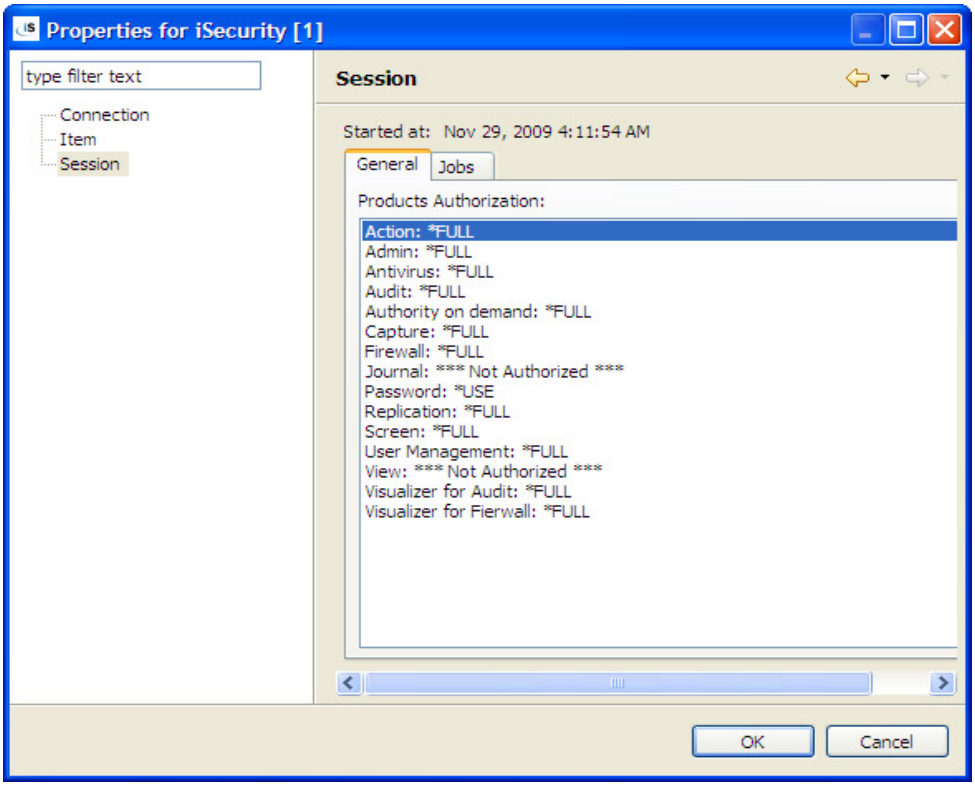
Item

Display node authorization and tag it for easier search of the specific item in the GUI application. Add a new tag or assign an existing one.



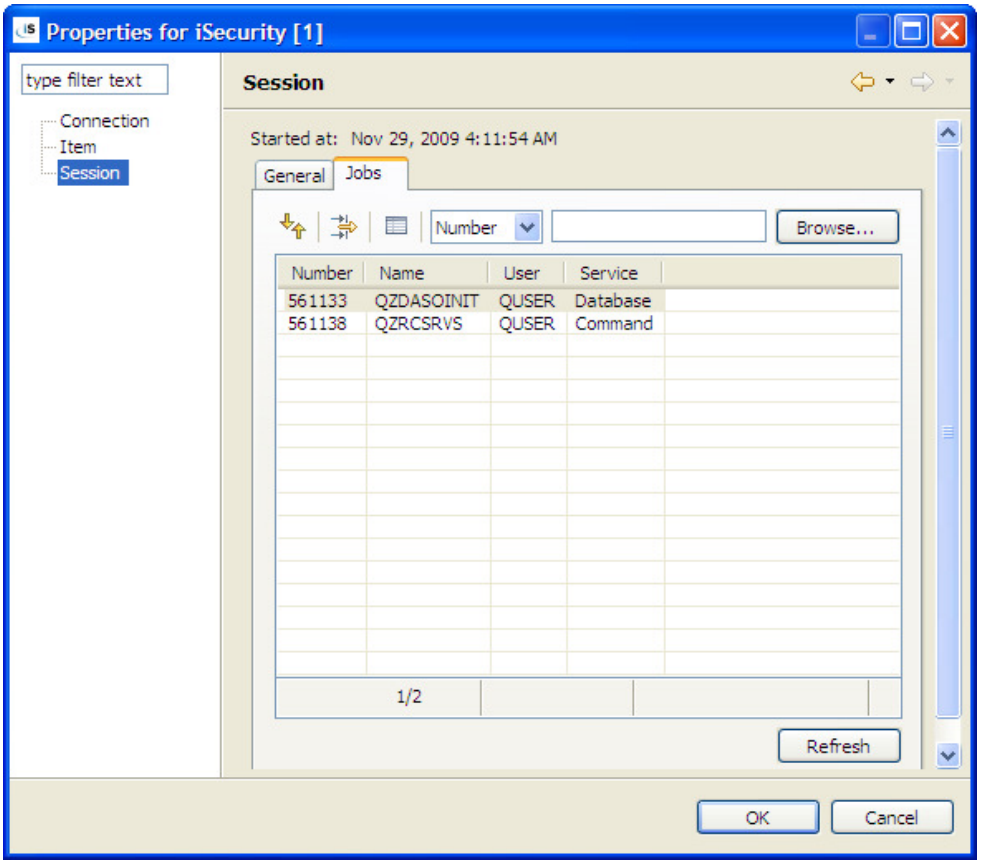
Session

Session lists product's authorization level



Session Properties - Session

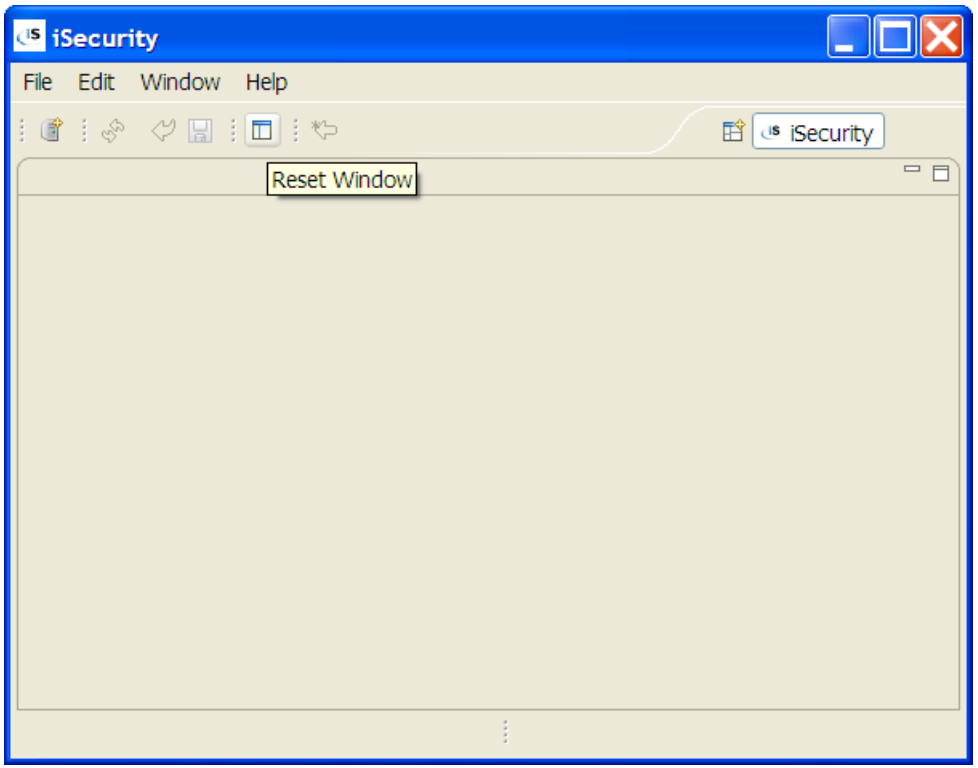
The Jobs tab lists session jobs



Session Properties - Jobs

Reset Window

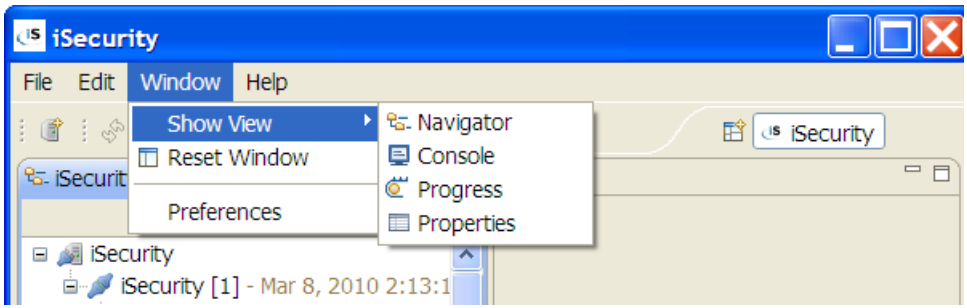
The GUI layout can easily restore it's state after it's being disposed, by using the **Reset Window** recovery button in the toolbar



Restore GUI Layout

Show View

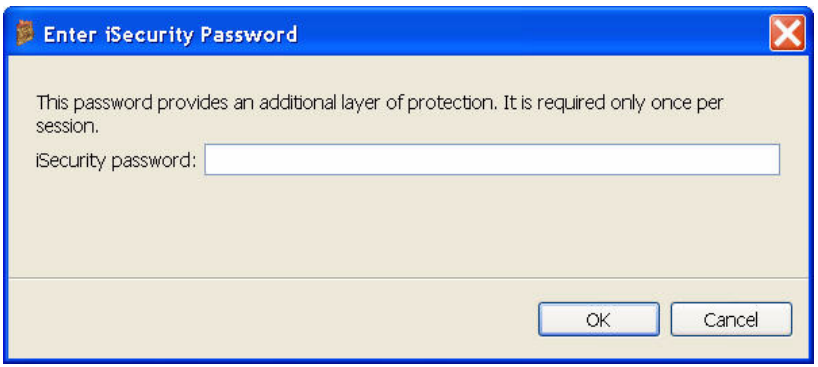
Select a view to display in the interface layout



Show View

Application Password

Application password is separated from connection data, which resembles the native side. Upon requesting data from the server the user is prompted for iSecurity password. Empty password is of course an option based on the user profile the user signed in with.

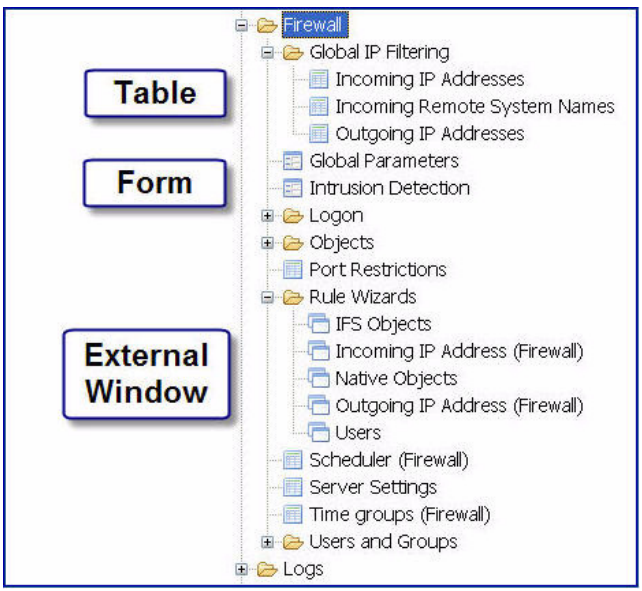

Enter iSecurity Password
This password provides an additional layer of protection. It is required only once per session.
iSecurity password:
OK
Cancel

Enter iSecurity Password

NOTE: *Unauthorized user will receive an error message*

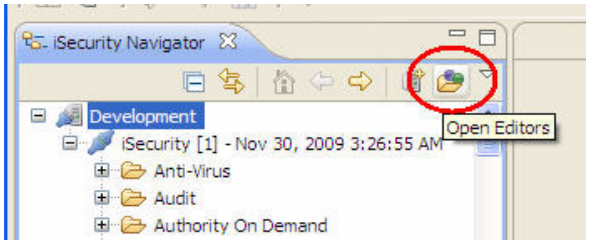
Screens and Editors

The navigator icons are differently designed according to what they display



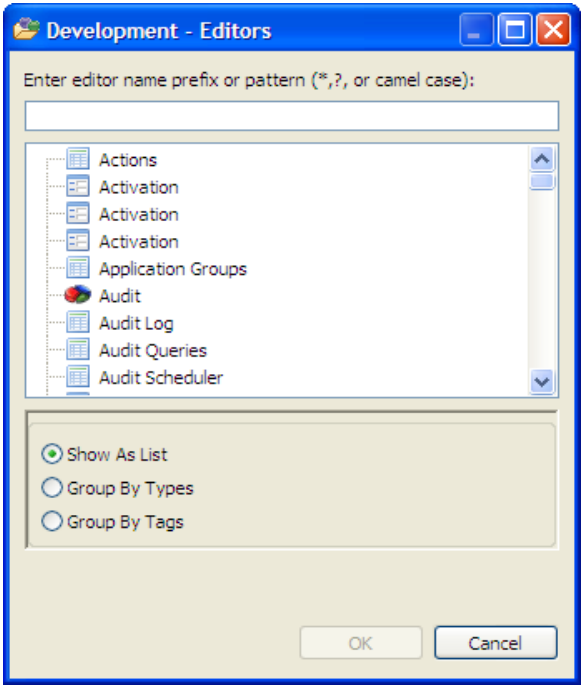
Editors

Click on “Open Editors” tool bar button to search editor name prefix or pattern



Open Editors

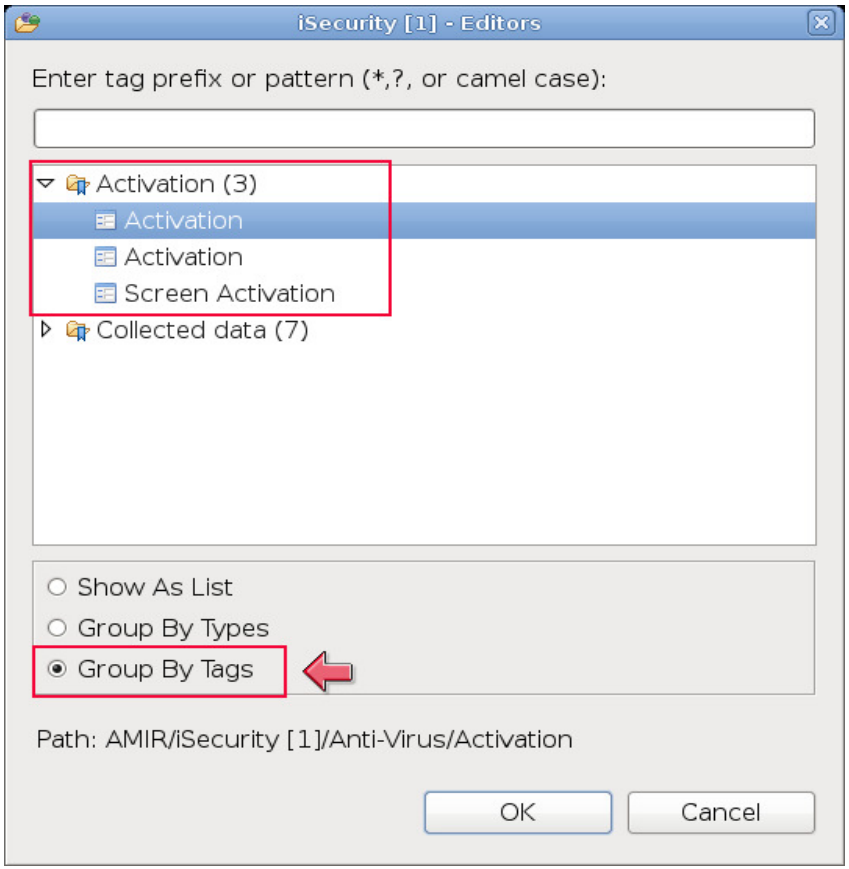
A list of editors appears in alphabetic order



Editors List

If **Group By Tags** is checked you can quickly activate selected editors.

This works also for multiple accounts/sessions



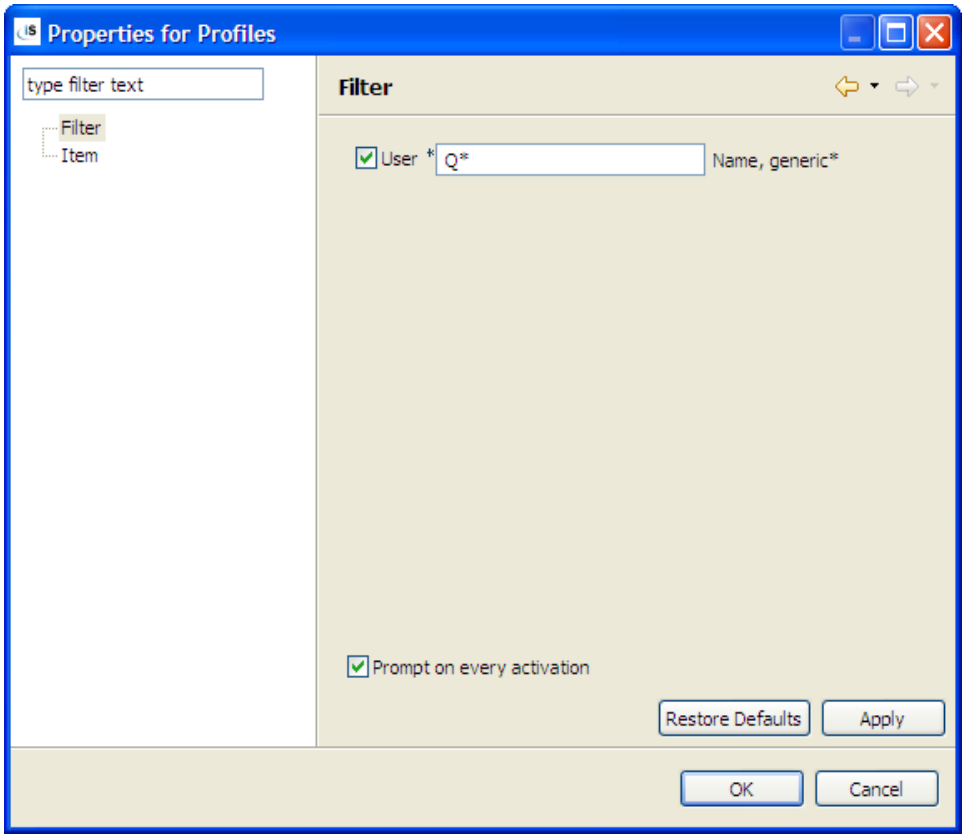
Editors List - by Tags

Nodes with filter

The following example use the **Profiles** node under **User Management**

To filter information, right-click the node, the properties dialog for **Profiles** displays, select **Filter**.

NOTE: *Changes done here will take place at the next attempt to open the editor or at the next attempt to refresh an already opened one.*

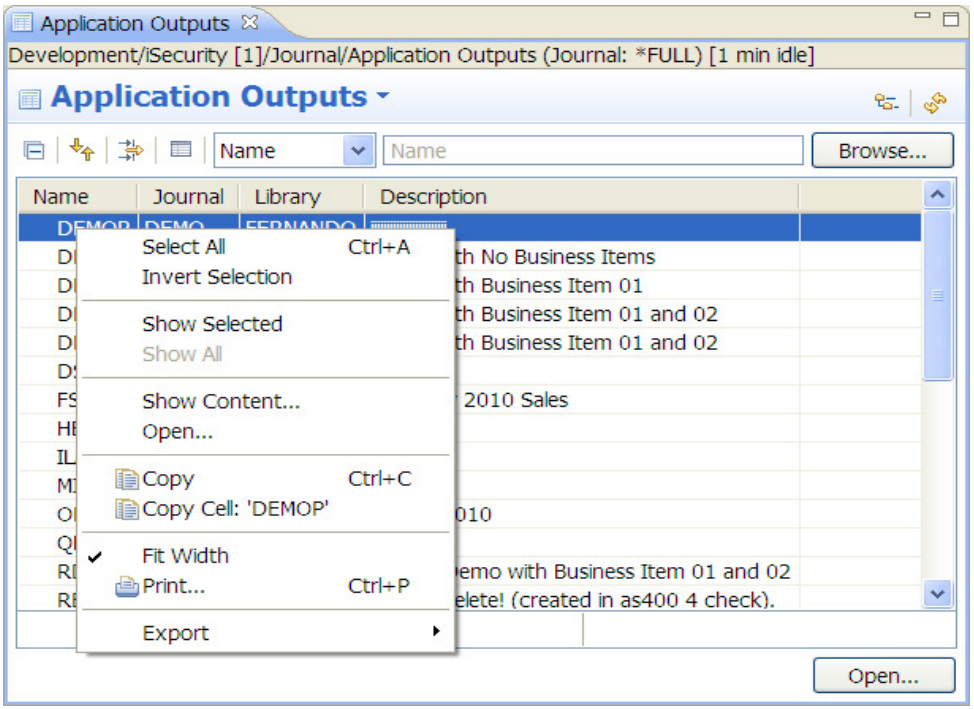


Properties Filter

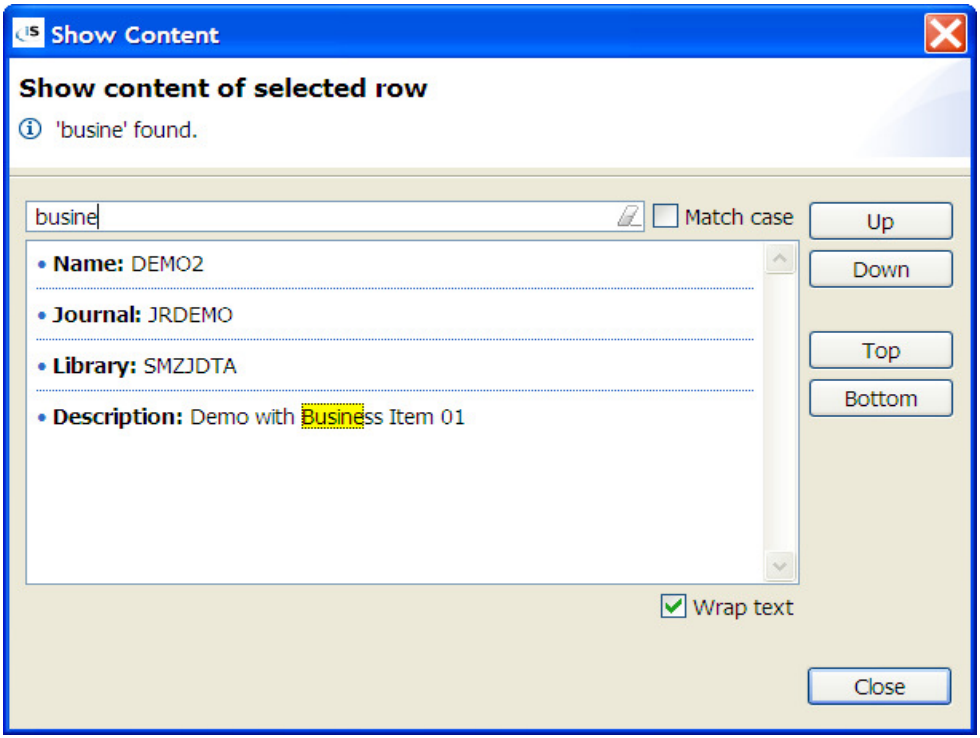
The filter is accessible also via editor's pop up

Show entry content

Right-click on any table record and select **Show Content** to view the table headers of the entry. This view will be the default view if the table has no **Open** button.



Show Entry Content



Show Content of Selected Row

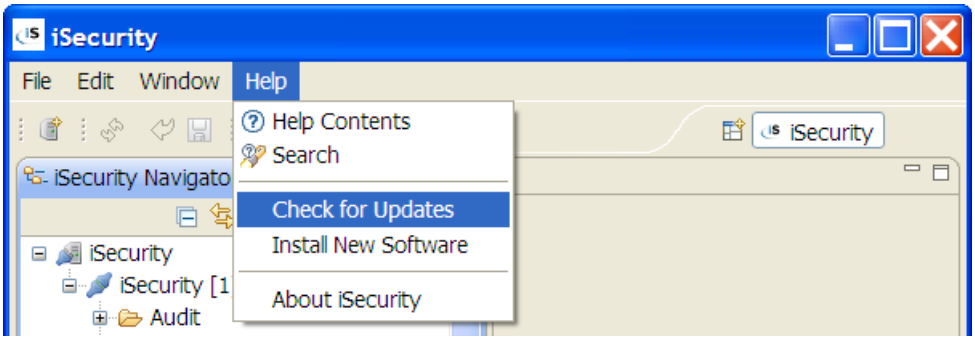
- Use the navigation buttons at the right to navigate the entries.
- Use the search bar at the top of the dialog box. The search string will be highlighted.

Update

Check for updates in one click

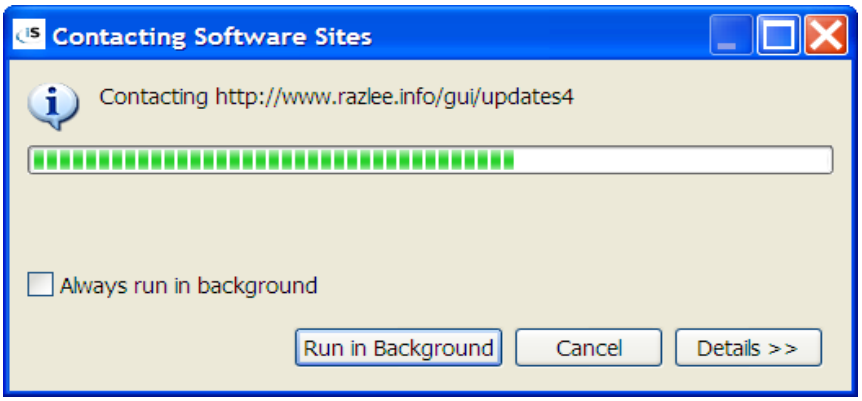
Updates and new releases are available through the GUI itself.

1. Go to **Help** -> **Check for Updates**



Check for Updates

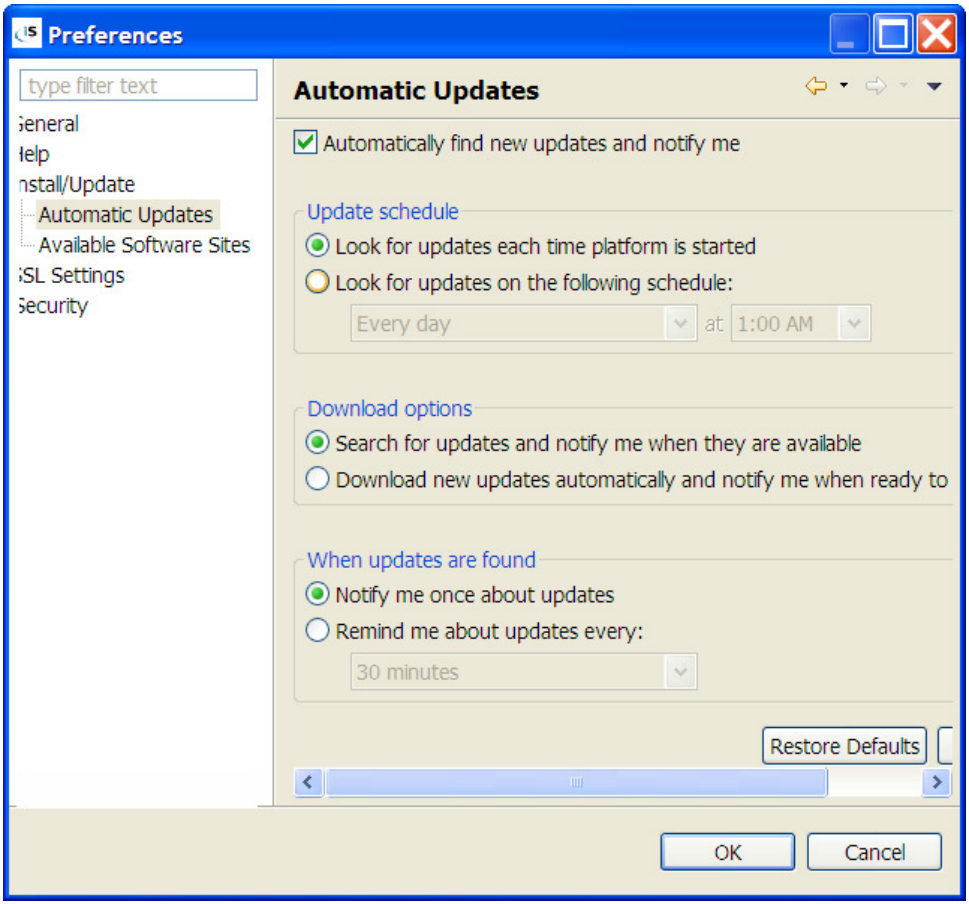
2. The GUI will automatically connect to the update site and perform the update



Contacting Software Site

Automatic and Scheduled Updates

1. To set automatic updates go to **Window -> Preferences -> Install/Update**
2. Check the **Automatically find new updates and notify me** check box, and set definitions



Automatic Updates

iSecurity Archived Update Site

If you don't have internet connection from the GUI, you can updated the application using a local update site.

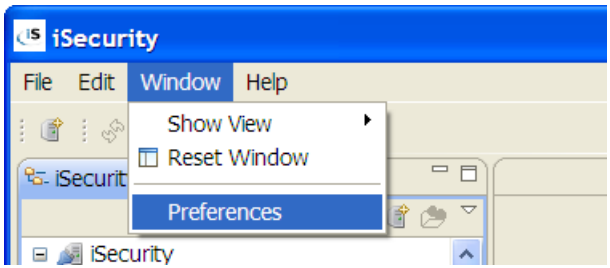
1. Ask for the new update zip file from your distributor and save it on your local disk.
2. Click **New Archived Site**
3. A "Select file" dialog will open, point it to the location of the zip file supplied to you.
4. On the "Edit Local Site" dialog click **OK**.

Reporting problems in iSecurity GUI

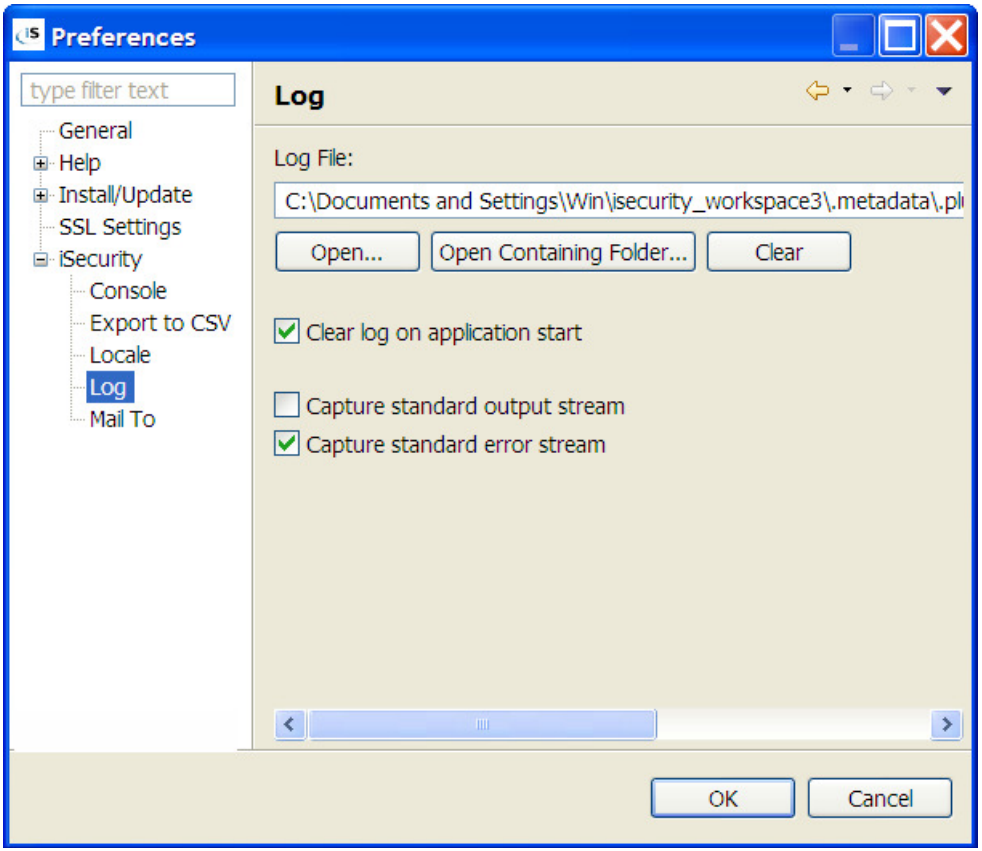
The iSecurity GUI module writes output to a log file. By default, problems are written to the log file which should be e-mailed to support@razlee.com .

Log Preferences window

1. Open the **Preferences** dialog from iSecurity's menu bar



2. Select **iSecurity** and click on the **Log** node



Preferences

NOTE: *Changes made on this screen take effect after iSecurity is restarted. By default, the log file is cleared when iSecurity starts and only errors are printed to it.*

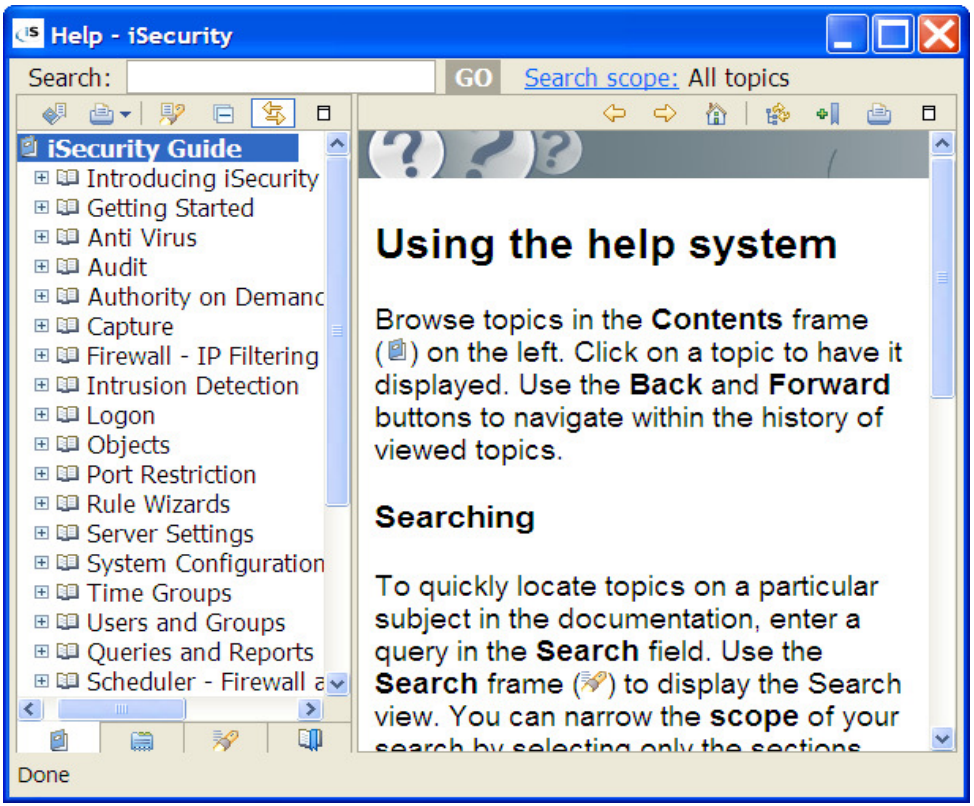
You may be asked by the Raz-Lee Technical Support team to check the "Capture standard output stream" box, re-create the error, and then re-send the log file to support@razlee.com .

Parameter	Description
Open	Opens the log file using the default text editor

Parameter	Description
Open Containing Folder	Useful if you wish to send the file as an attachment
Browse	Set a different log file location and name

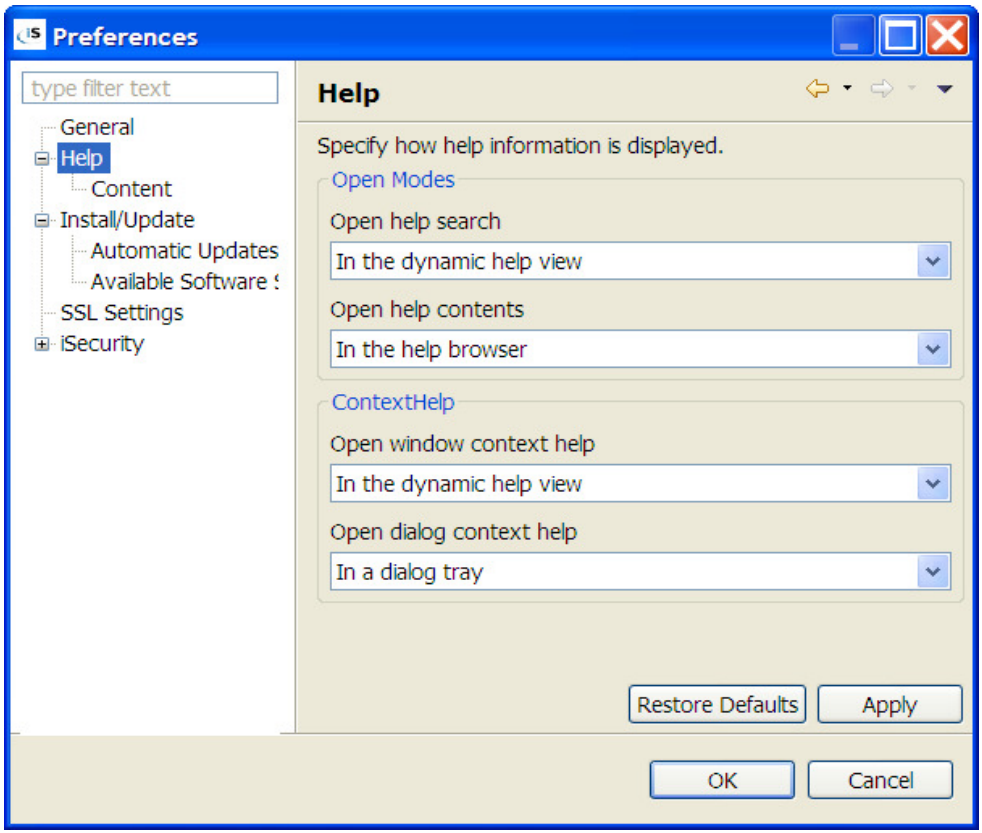
Help

A new Help contents available in HTML format that support links and bookmarks for easier navigation. The Help also support a search engine.


Help - iSecurity
Search:
GO
Search scope: All topics
iSecurity Guide
Introducing iSecurity
Getting Started
Anti Virus
Audit
Authority on Demanc
Capture
Firewall - IP Filtering
Intrusion Detection
Logon
Objects
Port Restriction
Rule Wizards
Server Settings
System Configuration
Time Groups
Users and Groups
Queries and Reports
Scheduler - Firewall a
Using the help system
Browse topics in the Contents frame ( ) on the left. Click on a topic to have it displayed. Use the Back and Forward buttons to navigate within the history of viewed topics.
Searching
To quickly locate topics on a particular subject in the documentation, enter a query in the Search field. Use the Search frame ( ) to display the Search view. You can narrow the scope of your
Done

Define Default Settings

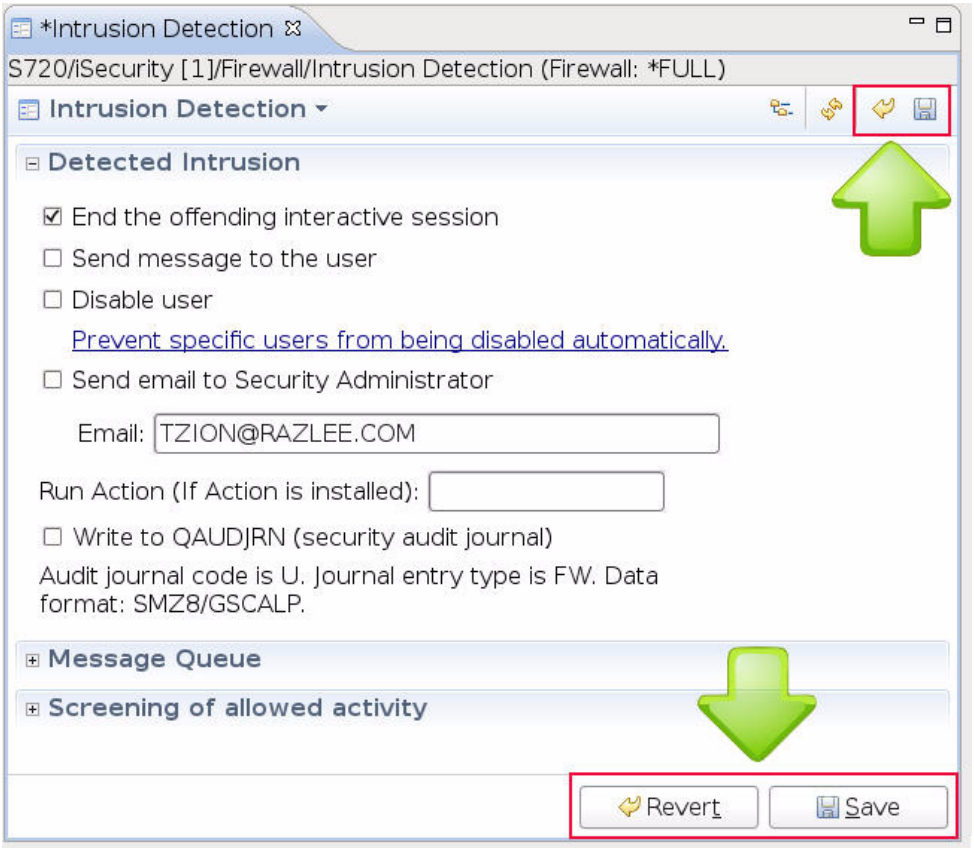
Go to **Window -> Preferences -> Help** and define the Help default settings



Help Preferences

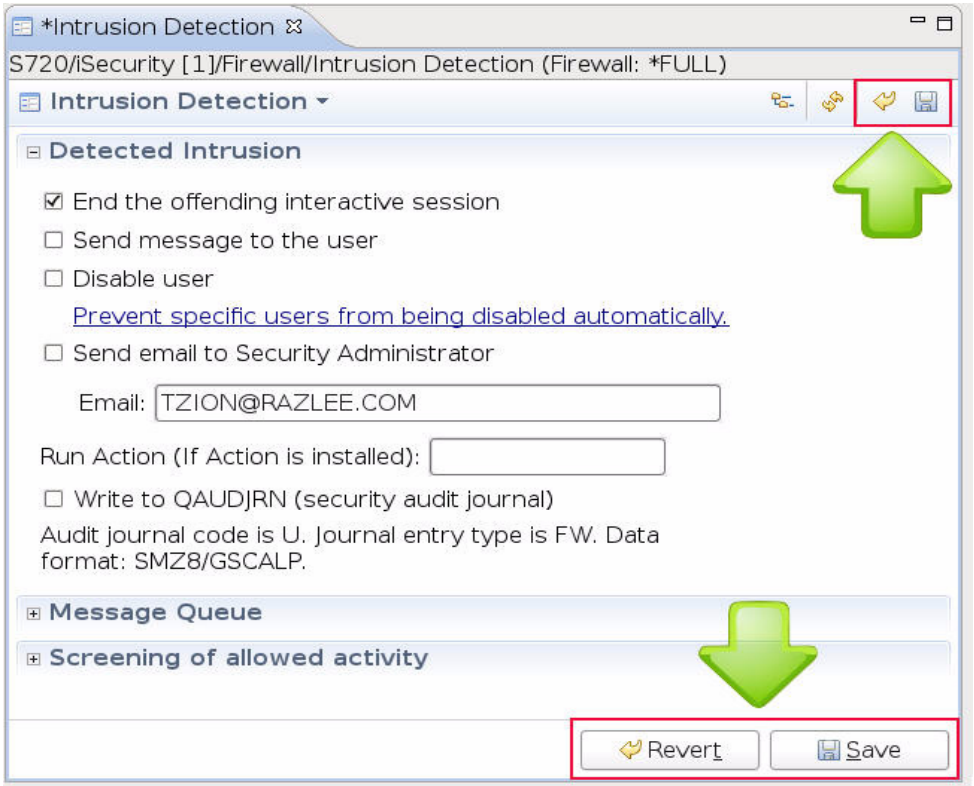
Editors

Most editors, whether forms or tables, have an internal tool bar which also shows load status


*Intrusion Detection
S720/iSecurity [1]/Firewall/Intrusion Detection (Firewall: *FULL)
Intrusion Detection
Detected Intrusion
End the offending interactive session
Send message to the user
Disable user
Prevent specific users from being disabled automatically.
Send email to Security Administrator
Email: TZION@RAZLEE.COM
Run Action (If Action is installed):
Write to QAUDJRN (security audit journal)
Audit journal code is U. Journal entry type is FW. Data format: SMZ8/GSCALP.
Message Queue
Screening of allowed activity
Revert
Save

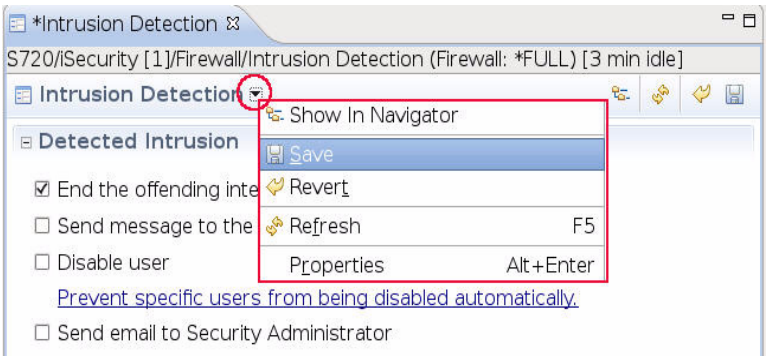
Editor Tool Bar

Every form has Save/Revert actions

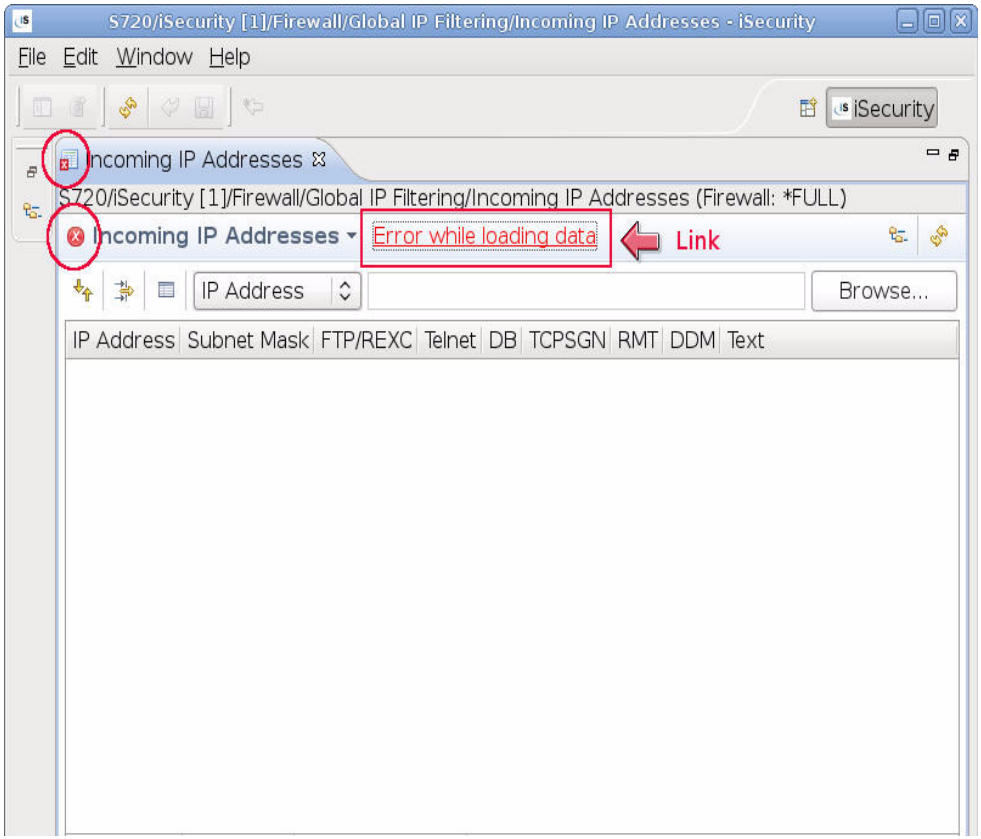

*Intrusion Detection
S720/iSecurity [1]/Firewall/Intrusion Detection (Firewall: *FULL)
Intrusion Detection
Detected Intrusion
End the offending interactive session
Send message to the user
Disable user
Prevent specific users from being disabled automatically.
Send email to Security Administrator
Email: TZION@RAZLEE.COM
Run Action (If Action is installed):
Write to QAUDJRN (security audit journal)
Audit journal code is U. Journal entry type is FW. Data format: SMZ8/GSCALP.
Message Queue
Screening of allowed activity
Revert
Save

Revert/Save

Editor's actions are available also via a pop up



Error messages as link

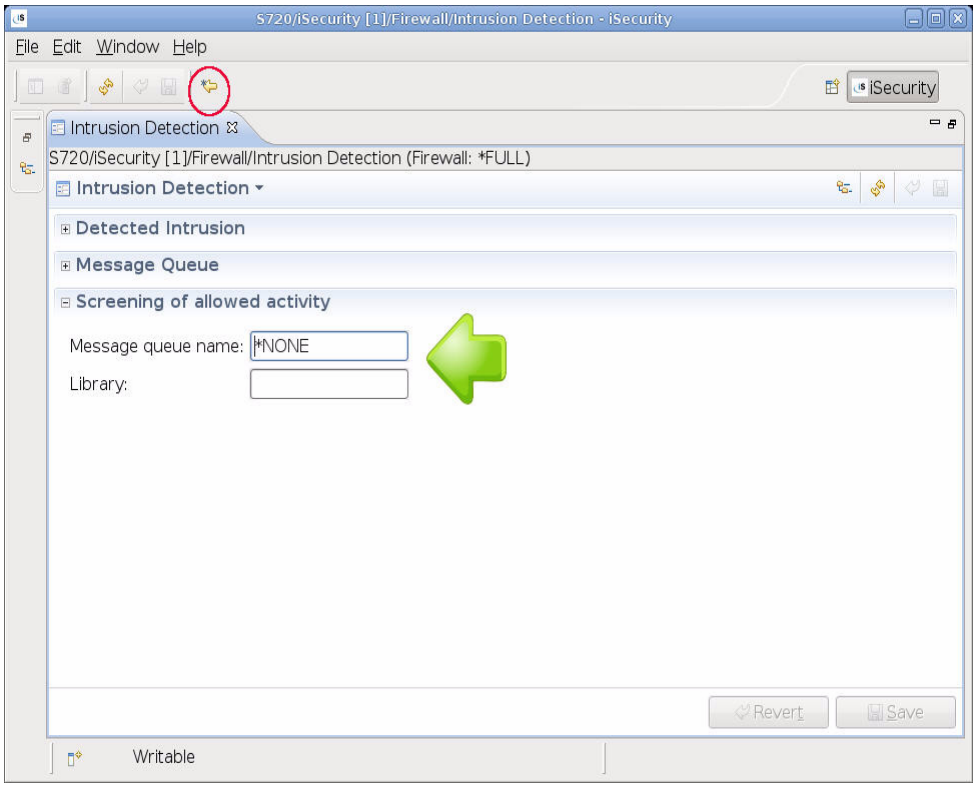

S720/iSecurity [1]/Firewall/Global IP Filtering/Incoming IP Addresses - iSecurity
File Edit Window Help
iSecurity
Incoming IP Addresses
S720/iSecurity [1]/Firewall/Global IP Filtering/Incoming IP Addresses (Firewall: *FULL)
Incoming IP Addresses
Error while loading data
Link
IP Address
Browse...
IP Address Subnet Mask FTP/REXC Telnet DB TCPSGN RMT DDM Text

Error messages as link

Clicking the link to display error message.

Last Modified Editor

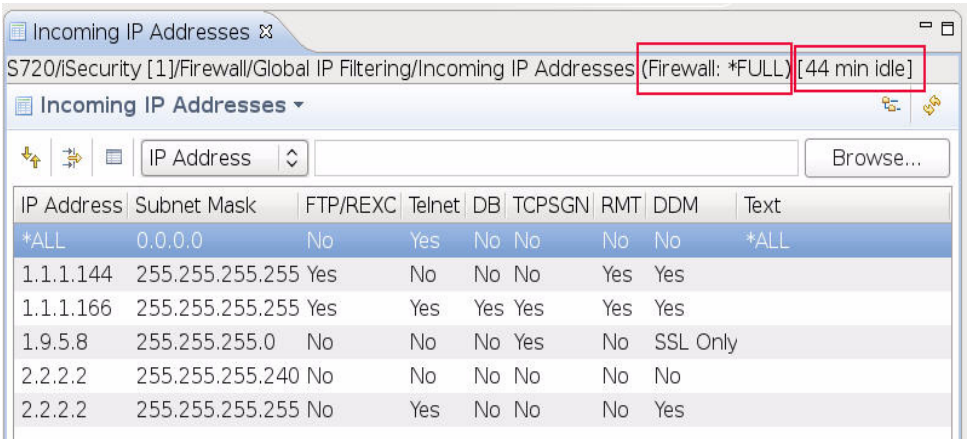
Last Modified Editor will activate the last form that has changed



Last Modified Editor

Editor Display

Editor displays product name, authorization information and idle time

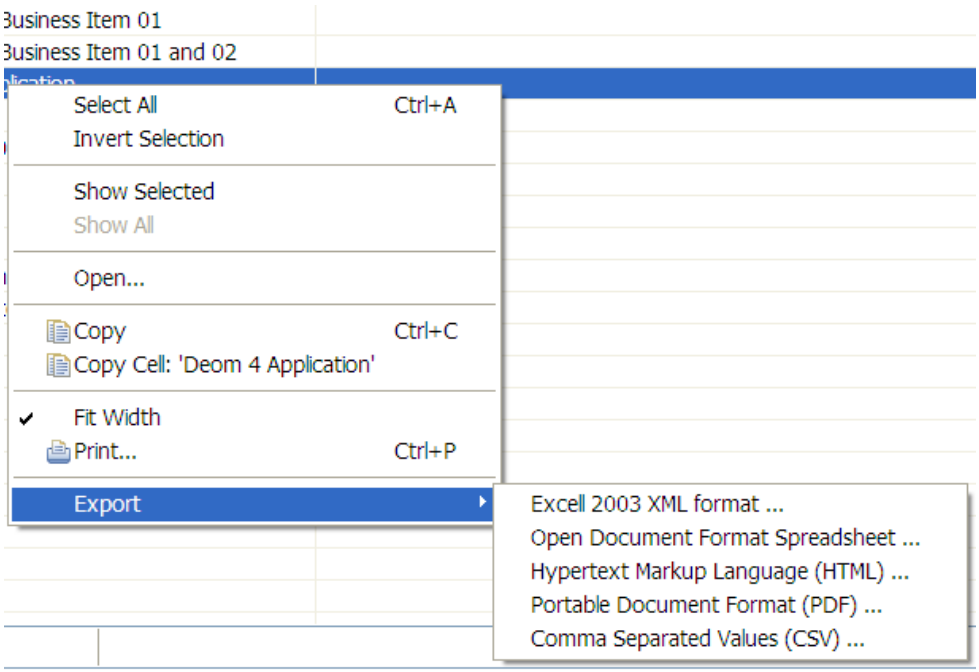

Incoming IP Addresses
S720/iSecurity [1]/Firewall/Global IP Filtering/Incoming IP Addresses (Firewall: *FULL) [44 min idle]
Incoming IP Addresses
IP Address
Browse...
IP Address Subnet Mask FTP/REXC Telnet DB TCPSGN RMT DDM Text
*ALL 0.0.0.0 No Yes No No No No *ALL
1.1.1.144 255.255.255.255 Yes No No No Yes Yes
1.1.1.166 255.255.255.255 Yes Yes Yes Yes Yes Yes
1.9.5.8 255.255.255.0 No No No Yes No SSL Only
2.2.2.2 255.255.255.240 No No No No No No
2.2.2.2 255.255.255.255 No Yes No No No Yes

Editor display

Print format

Right-click on a records or several records to print in the following printing formats:

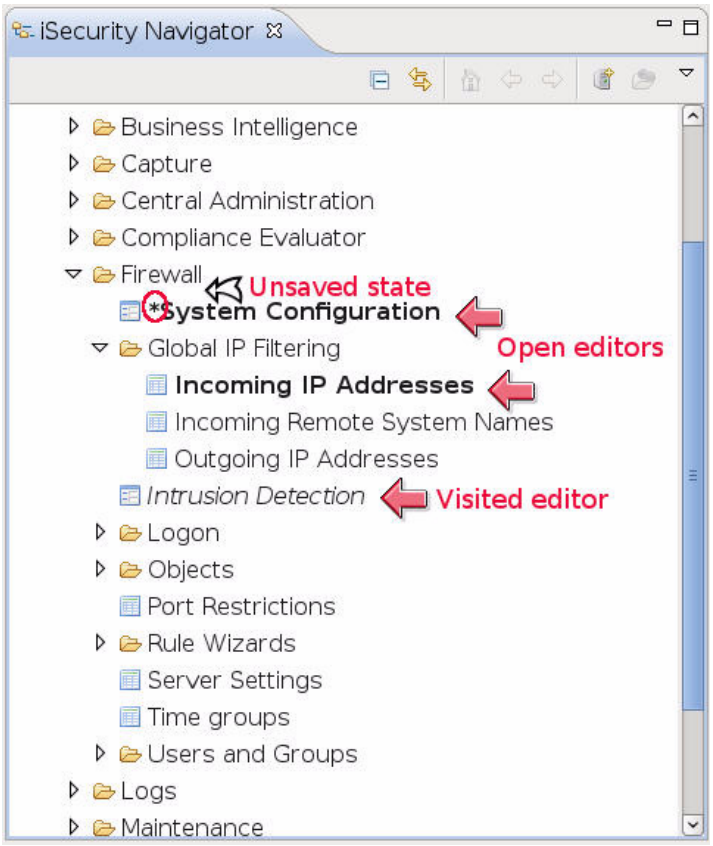
- Print to a printer
- Select “Fit Width” to print the entire record on a single page
- Select “Export” to export records to five different formats: Excel, Open Source Spreadsheet, HTML, PDF and CSV.



Print Formats

Open editor display

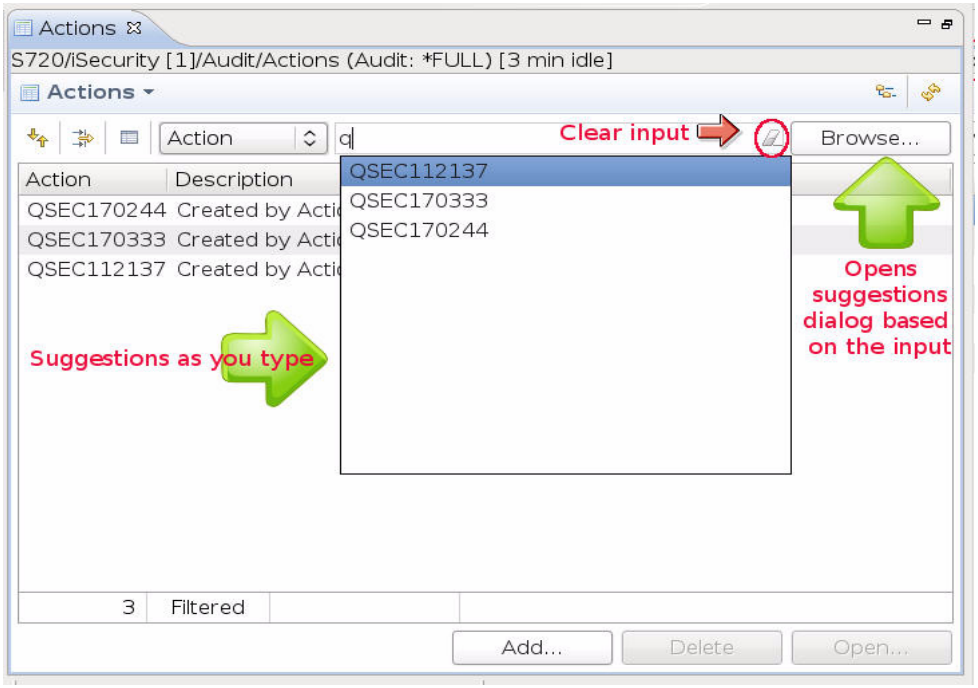
Open editors have special rendering in the Navigator View and appears in Italics.



Open Editors Display in Navigator View

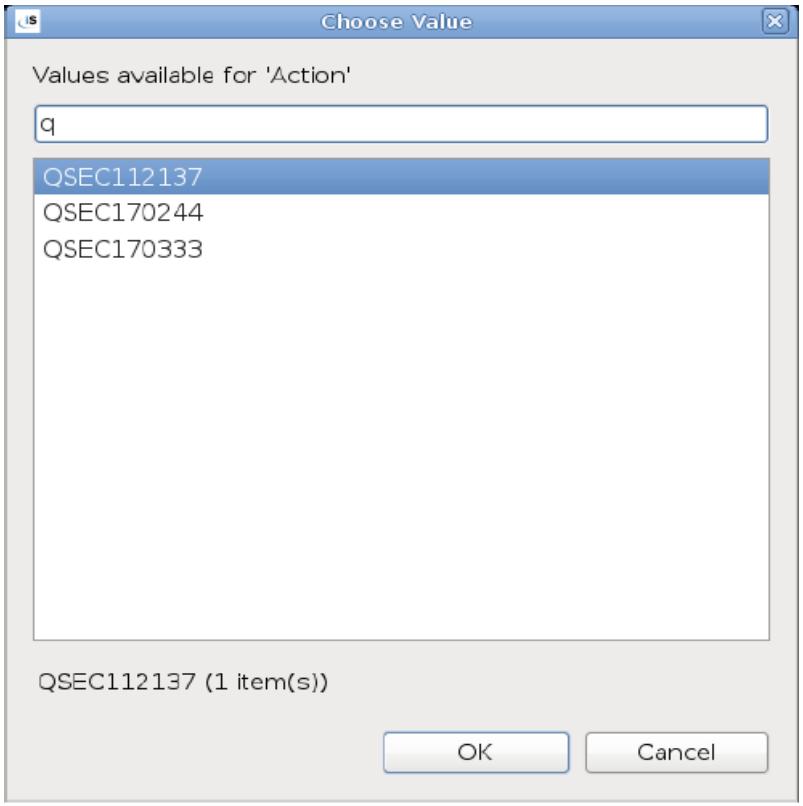
Editor Filter

All editors have a built in filter that also suggest filter criteria



Editor Filter

Click Browse to open the suggestions dialog box based on the input



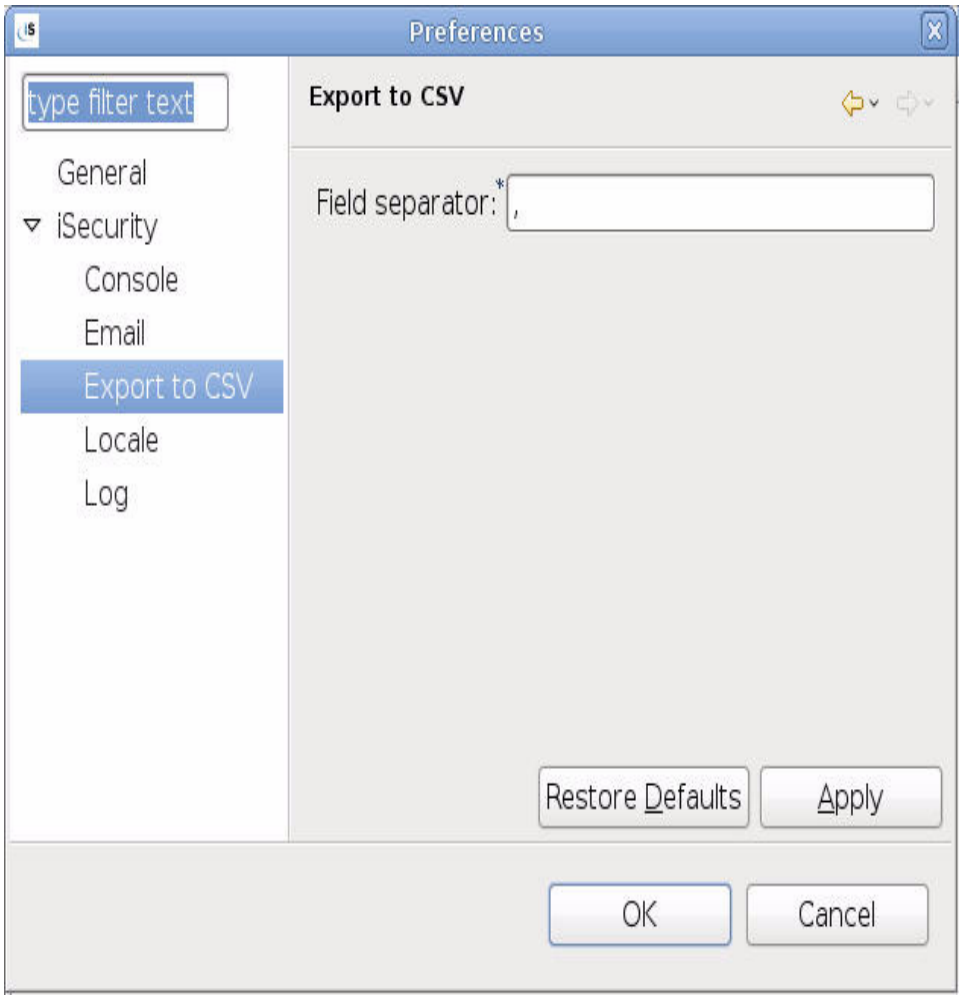
Suggestions Dialog

Rule Wizards

Every rule wizard has a Data set configuration button

Data set configuration

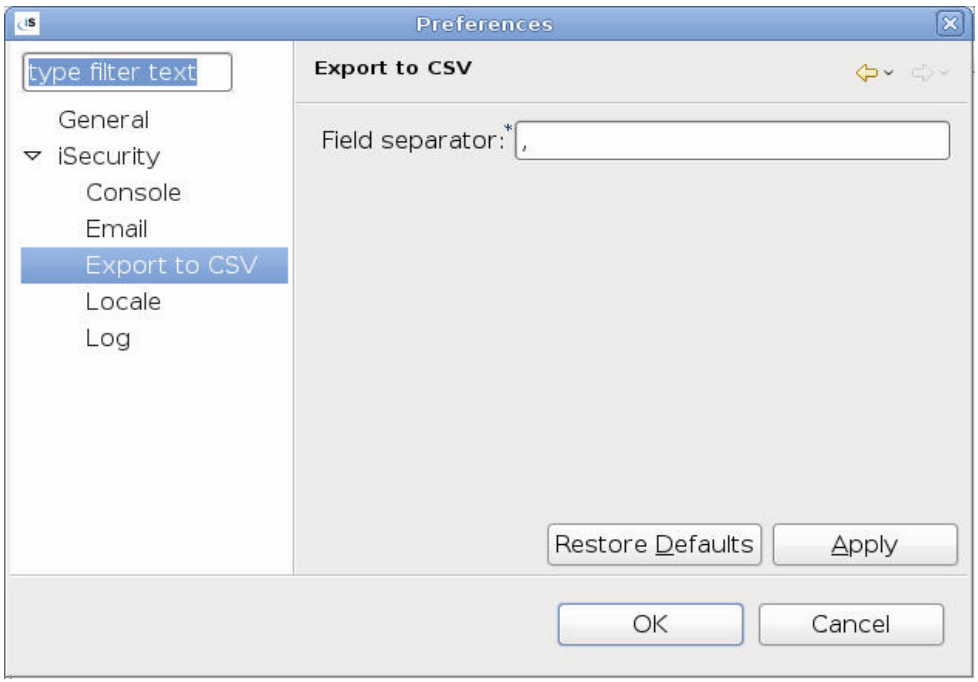
The command prompter for data set configuration



command prompter

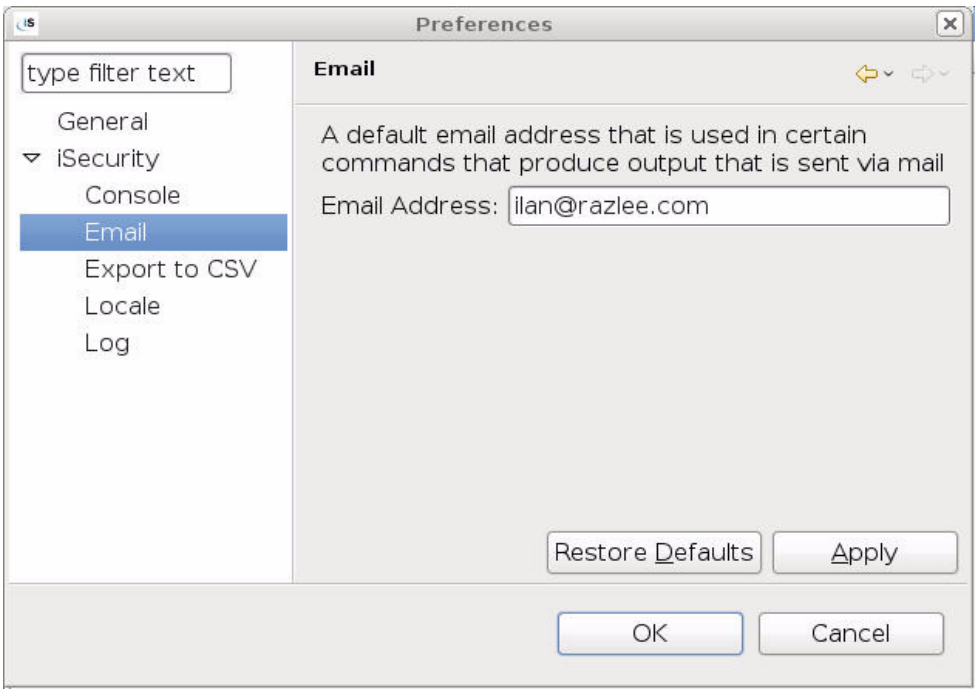
Preferences

Setting field separator for CSV outputs (used in the logs)



Field Separator for CSV

A default E-mail address to be used in queries, compliance and scheduler



Default E-mail Address

3 AP-Journal

Chapter 3: AP-Journal

Workflow

The following workflow explains how to work with the GUI version of **AP-Journal:**

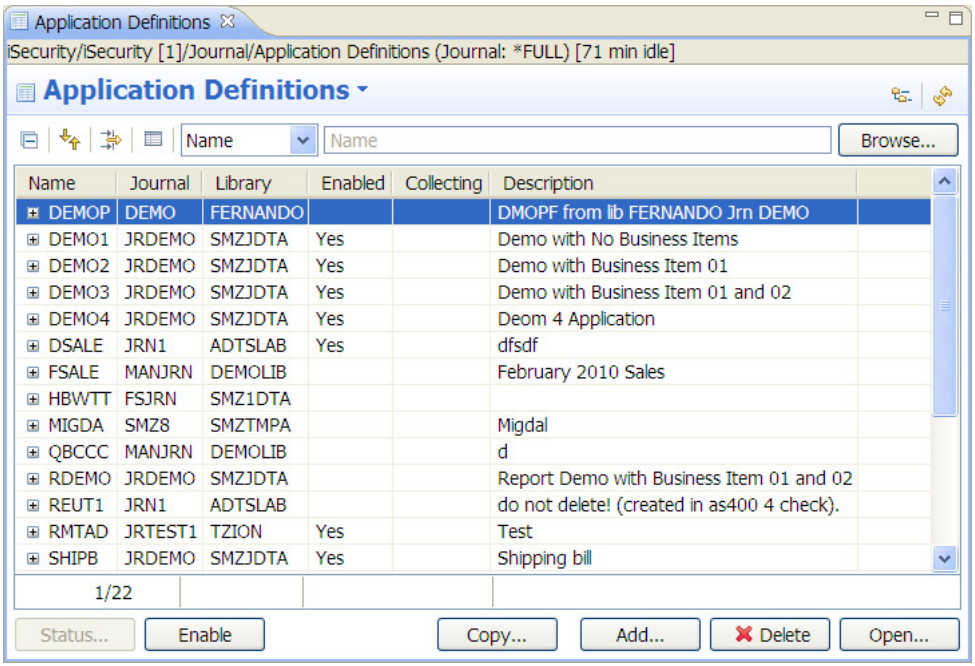
1. Define Application
   - If this is a new application
     - Add Application: select journaled file, define Business Items
     - Add files to the application
     - Set file definitions: define alerts before filter (define Business Alerts Actions), set filter definitions, define alerts on data after filter
   - If this is an existing application you wish to edit
     - Select application, define/edit Business Items, add Visualizer latest data
     - Add files to the application or Set file definitions
2. Collecting Data
   - Enable the application
   - Status of data collection
3. Add latest data to the Visualizer Maintenance

Application Definitions

In order to view files and fields' changes from several files, create an application of files that will join information from all the relevant files and fields needed. After creating the application, the first ***Container*** will create automatically. This ***Containe***r contains the same logical information from the system's ***receiver***, in a filtered format from the files and fields you chose. In that way, only the relevant information will be kept in the system.

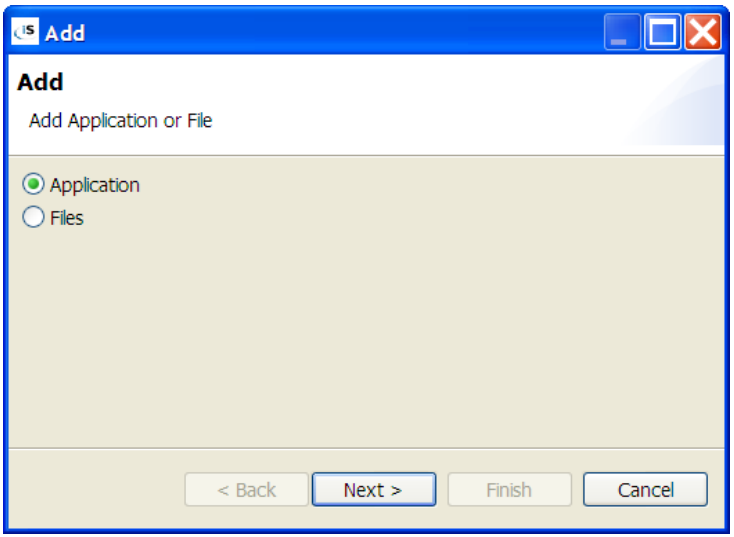
Adding Application

1. Open the **AP-Journal** node and double-click **Application**

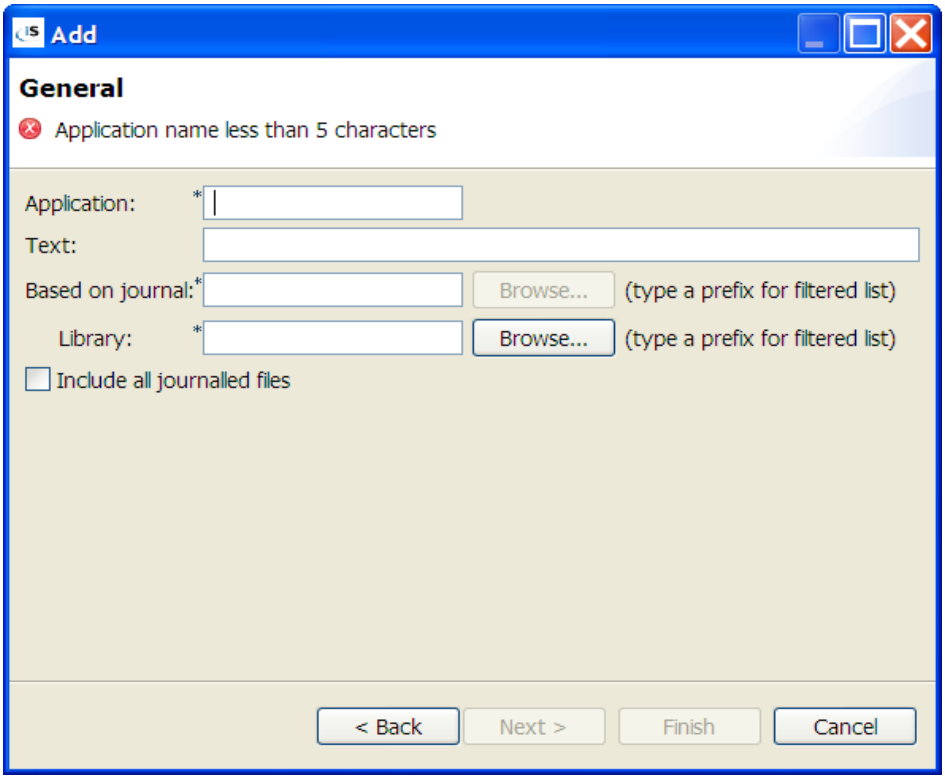

Application Definitions
iSecurity/iSecurity [1]/Journal/Application Definitions (Journal: *FULL) [71 min idle]
Application Definitions
Name
Name
Browse...
Name Journal Library Enabled Collecting Description
DEMOP DEMO FERNANDO DMOPF from lib FERNANDO Jrn DEMO
DEMO1 JRDEMO SMZJDTA Yes Demo with No Business Items
DEMO2 JRDEMO SMZJDTA Yes Demo with Business Item 01
DEMO3 JRDEMO SMZJDTA Yes Demo with Business Item 01 and 02
DEMO4 JRDEMO SMZJDTA Yes Deom 4 Application
DSALE JRN1 ADTSLAB Yes dfsdf
FSALE MANJRN DEMOLIB February 2010 Sales
HBWTT FSJRN SMZ1DTA
MIGDA SMZ8 SMZTMPA Migdal
QBCCC MANJRN DEMOLIB d
RDEMO JRDEMO SMZJDTA Report Demo with Business Item 01 and 02
REUT1 JRN1 ADTSLAB do not delete! (created in as400 4 check).
RMTAD JRTEST1 TZION Yes Test
SHIPB JRDEMO SMZJDTA Yes Shipping bill
1/22
Status...
Enable
Copy...
Add...
Delete
Open...

AP-Journal Application

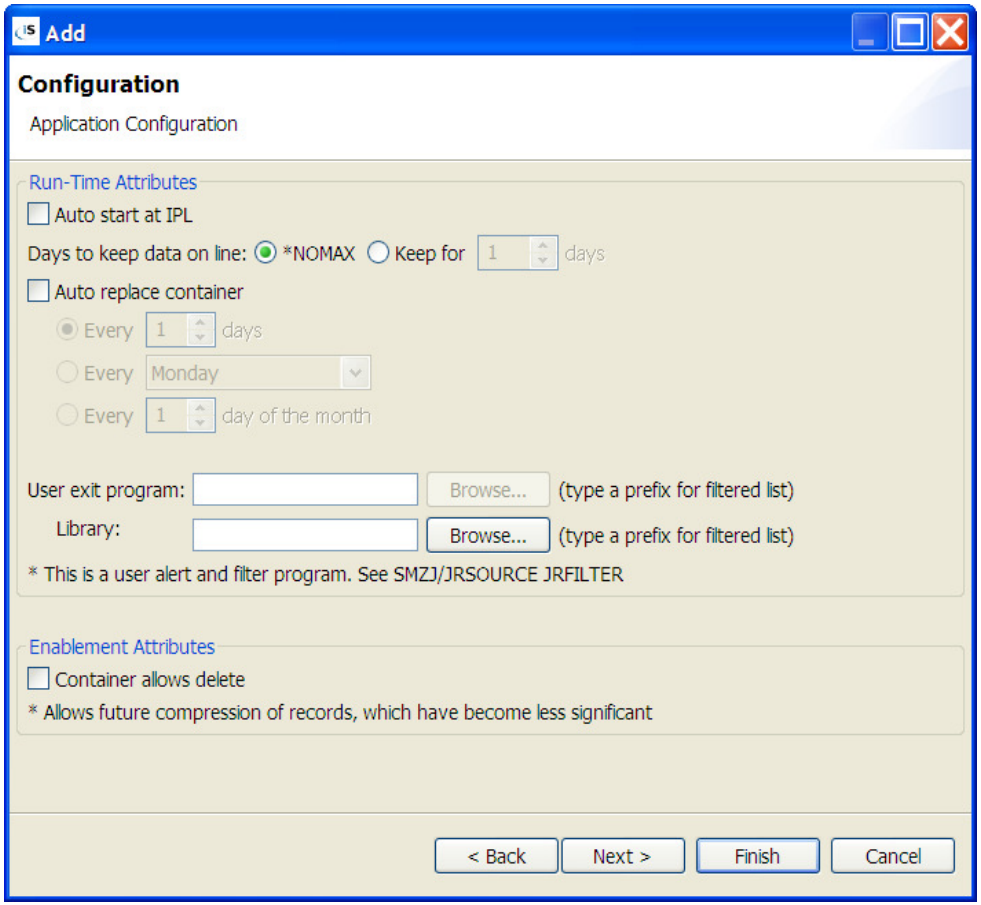
2. Click **Add** to add a new application or **Open** to modify and existing one



Add a New Application



Application General Definitions


Add
Configuration
Application Configuration
Run-Time Attributes
Auto start at IPL
Days to keep data on line: *NOMAX Keep for 1 days
Auto replace container
Every 1 days
Every Monday
Every 1 day of the month
User exit program: Browse... (type a prefix for filtered list)
Library: Browse... (type a prefix for filtered list)
* This is a user alert and filter program. See SMZJ/JRSOURCE JRFILTER
Enablement Attributes
Container allows delete
* Allows future compression of records, which have become less significant
< Back
Next >
Finish
Cancel

Add Application Configuration

NOTE: *In case Raz-Lee's* **FileScope** *in installed, it's journal file can be used. The file name is:* **FSJRN** *at library:* **SMZ1DTA**.

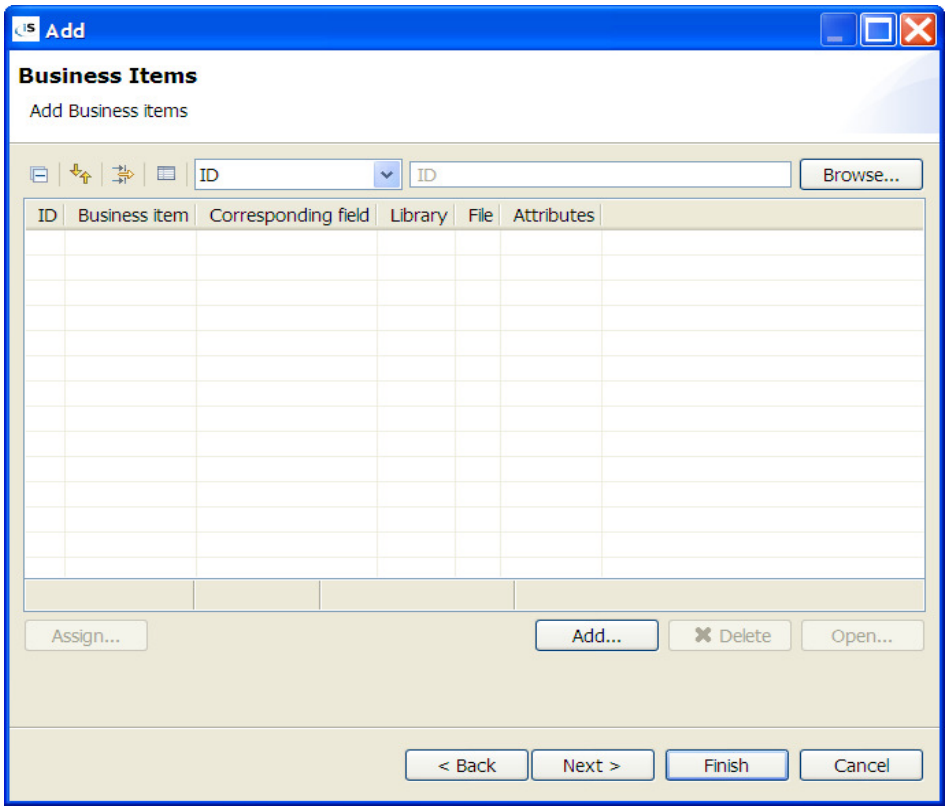
3. The following table will provide an explanation of the options:

Option	Description
Application	Insert five character application name
Text	Insert descriptive text
Based on journal	Insert the system's journal file and library name

Option	Description
Include all journaled files	Check the box to include all the journaled files or uncheck it and select specific files to include using option **1. Files to include** below.
Auto Start at IPL	Select number of days to keep data online and to auto replace container
User Exit Program	Type a name and library of a ready made program containers predefined alerts and filter conditions
Enablement Attributes	Container allows delete

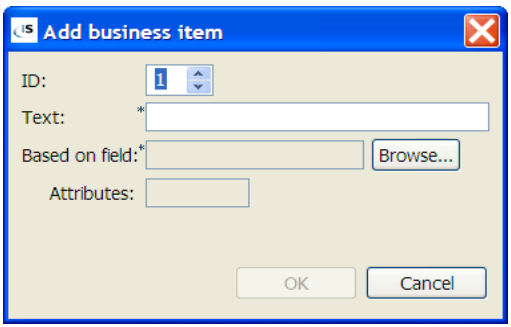
4. Click **Next** to add **Business Items** to the application definitions

Business Items are common key fields which contain the same information across several files in the application. Usually they are generic key fields. Such fields can later be used for selections.
For each application you can select up to 15 fields.



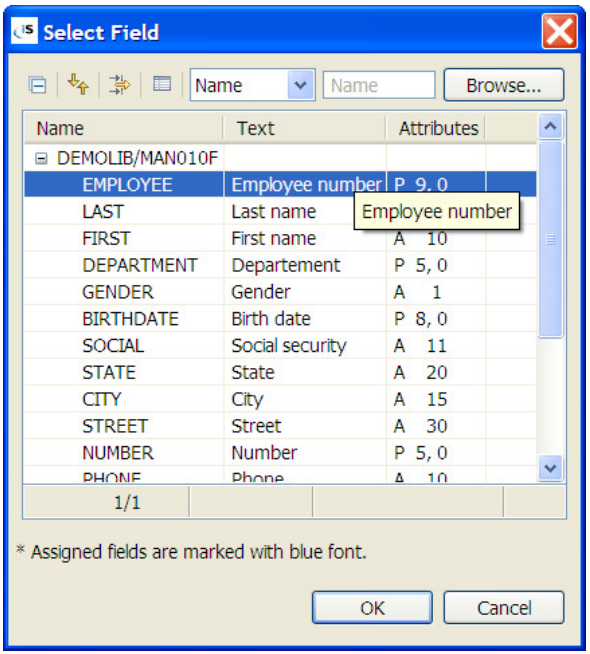
Add a Business Item

5. Click **Add**. The **Add Business Item** screen appears



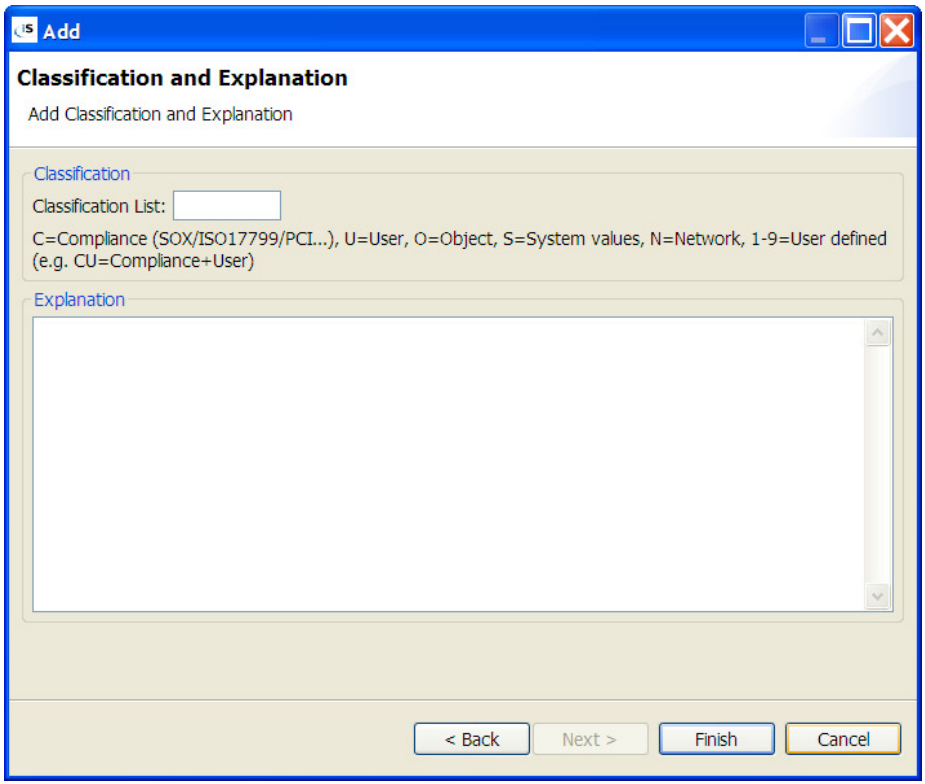
Add Business Item

6. Select ID number, type the Business Item text, Select a field to base on and click **OK** to continue. Click Browse to select from a list of fields



Select Field

7. Select more than one attribute by pressing CTRL. The selected attributes will appear in blue. The **Classification and Explanation** screen appears

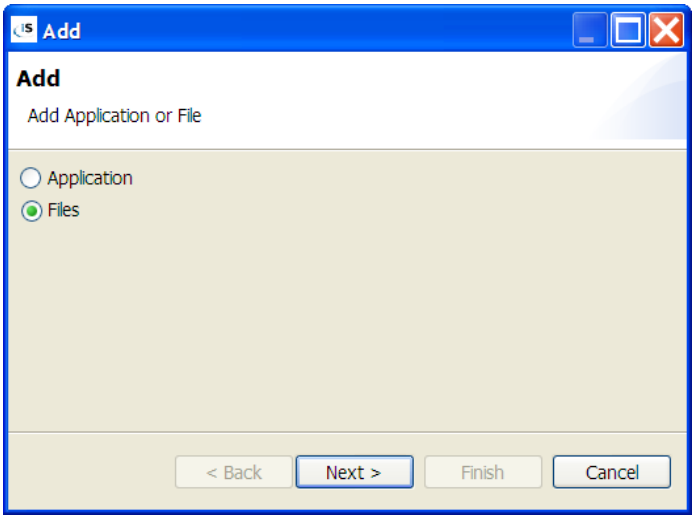


Add a Business Item - Classification and Explanation

8. Add classification and explanation tags for search condition and click **Finish** to create the new application.
9. Open the application again, select the **Business Items** tab and click **Assign**

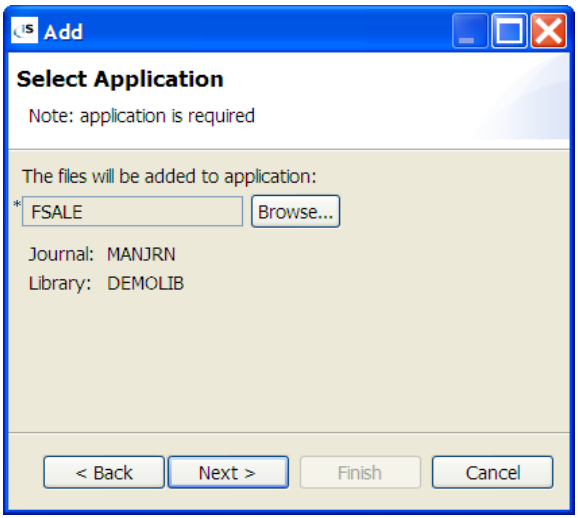
Add File to the Application

1. Click **Add** to add files to application



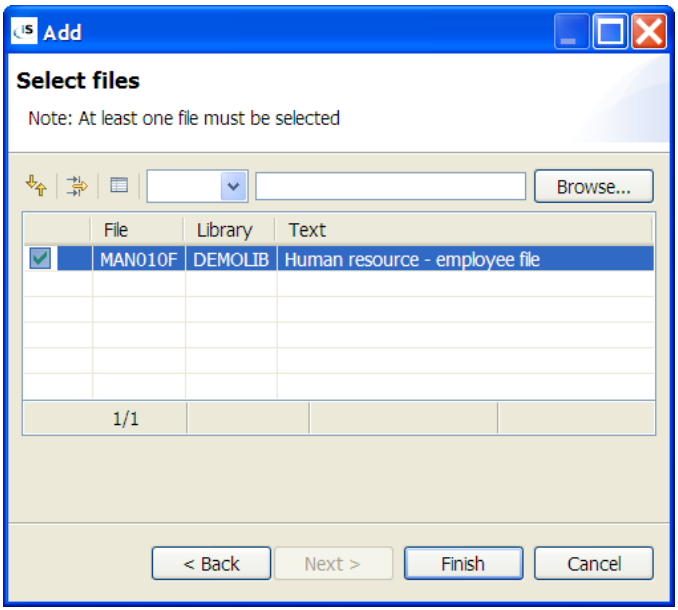
Add File

2. Select **Files** and click **Next**



Select Application

3. Type an application name or browse to select from a list, and click **Next**

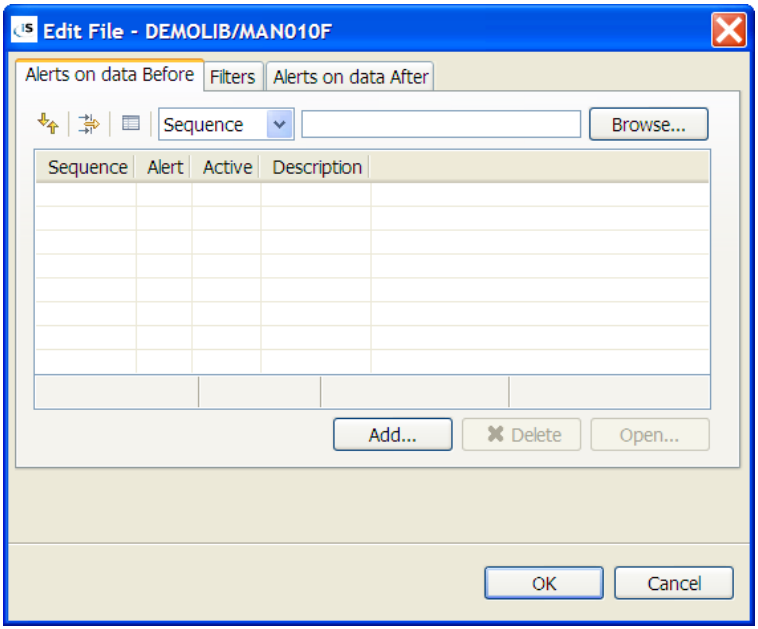


4. A list of files appears, select a file to add to the application and click **Finish**. The file will be added to the application.

Set File Definitions

Add alerts and filter definitions to the application on the file level.

Select a file in an application, and click **Open**

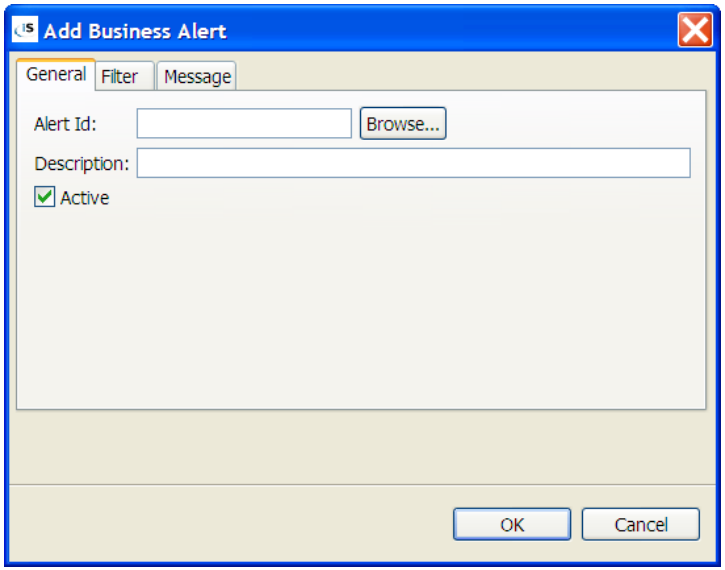


Edit File

Alerts on data Before

Define alerts based upon the changes in the journal receiver before filter definitions are checked

1. Click **Add**

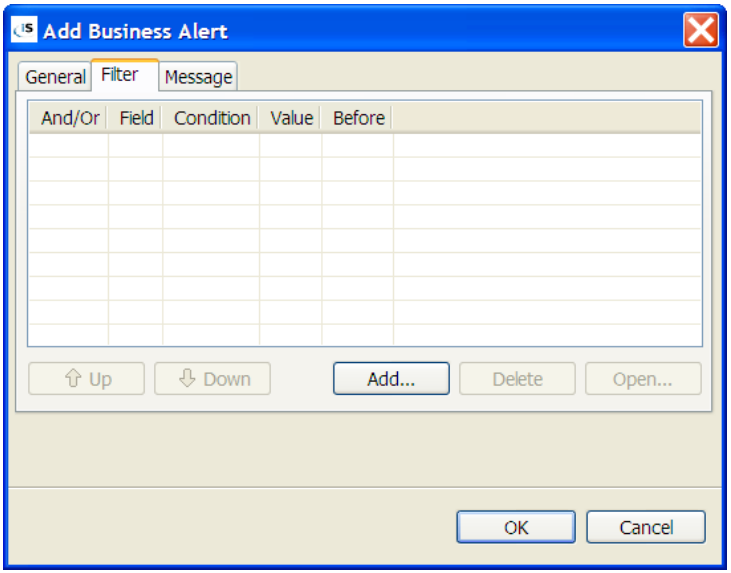


Add Business Alert

2. Type **Alert ID** or click **Browse** to select from a list.

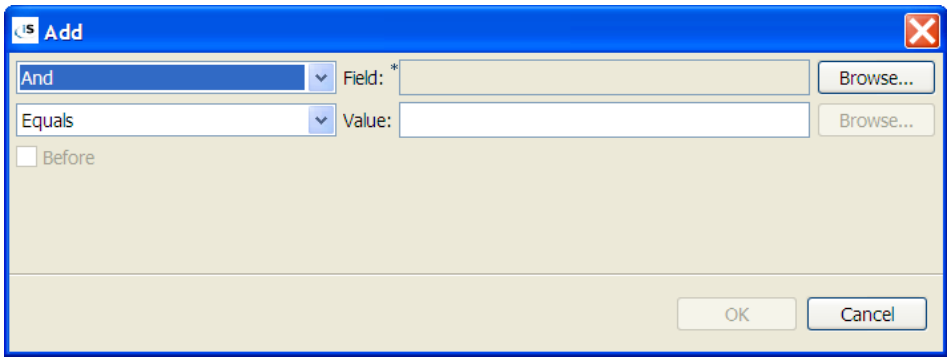
   NOTE: *To add a new action see* **page 70**.

3. Type a descriptive text at the **Description** field
4. Check **Active**
5. Click **Filter** tab to add filters to the alert



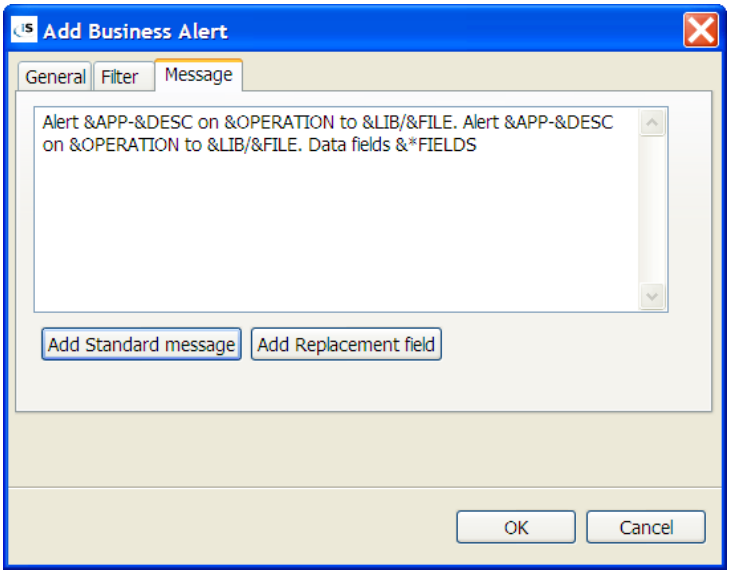
Add Business Alerts - Filter

6. Click **Add** to add filter conditions



Add Filter

7. Select conditions, fields and values. Click Browse to select from a list. Click OK to confirm.
8. Select Message tab to define the alert message



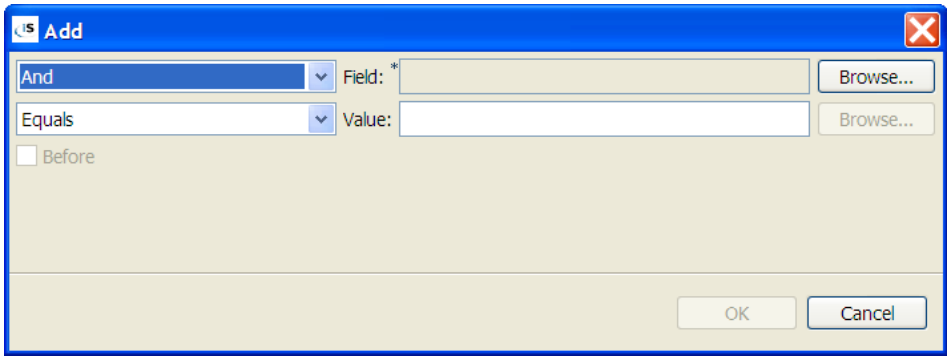
Alert Message

9. Click **OK** to continue

Filters

Select the file **Filter** tab define filters to the file data.

1. Click **Add**



Add Filter

2. Select conditions, fields and values. Click **Browse** to select from a list. Click **OK** to confirm.

Alerts on data After

Select the **Alerts on data After** tab to define real-time action based on changes in the containers data after the filter definitions were checked.

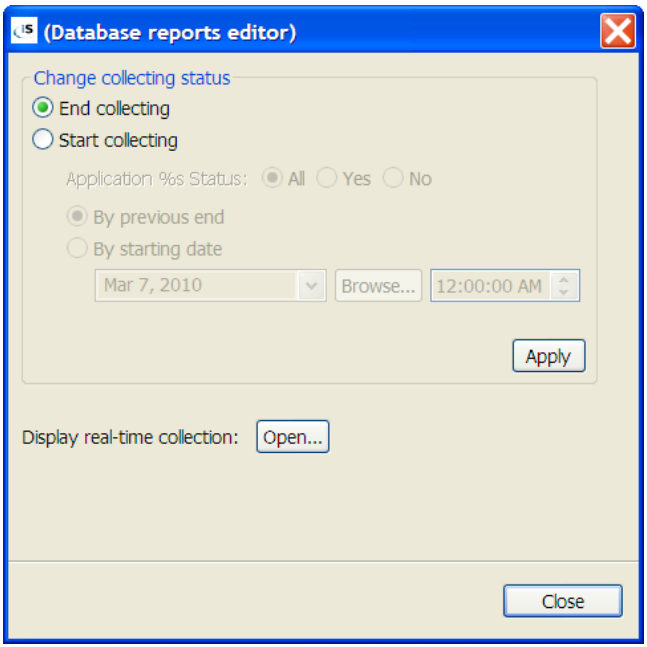
See *Alerts on data Before* above procedure

Enable Application

After creating and defining the new application, click **Enable** to start building the definitions file.

Status

Click **Status** to view the collection status of the application.



Status

Select **Start Collecting**, application reads the definition file and builds subsystem which collects the data (**By Previous end** = from beginning of available data or from today).

A blue "Yes" will appear in the collecting field

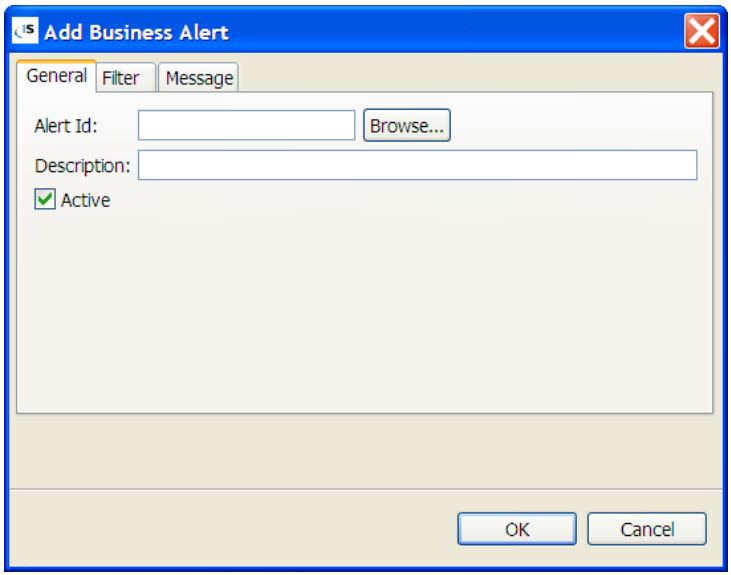
Name	Journal	Library	Enabled	Collecting	Description
⊞ DEMO4	JRDEMO	SMZJDTA	Yes		Deom 4 Application
⊞ DSALE	JRN1	ADTSLAB	Yes	Yes	dfsdf
⊞ FSALE	MANJRN	DEMOLIB			February 2010 Sales

Collecting Status

Add a New Action

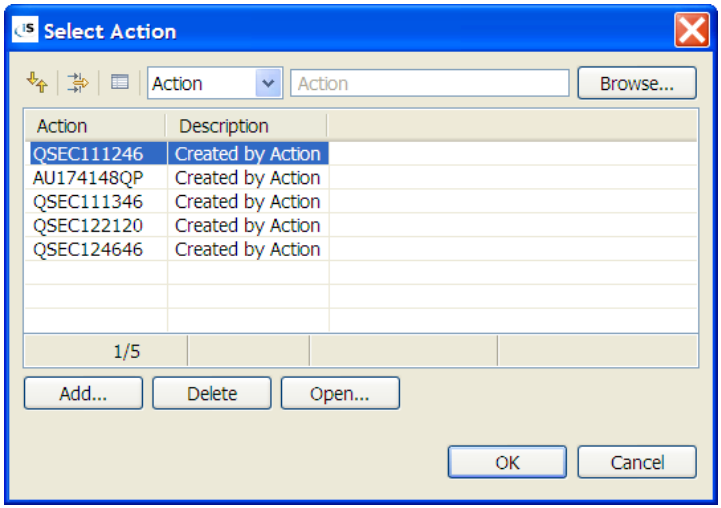
To add a new action, to be triggered according to a specified rule, follow this procedure:

1. Select an application's file, and click **Open**
2. Select **Alerts on Data Before/After** tab and click Add. The **Add Business Alerts** dialog box appears.



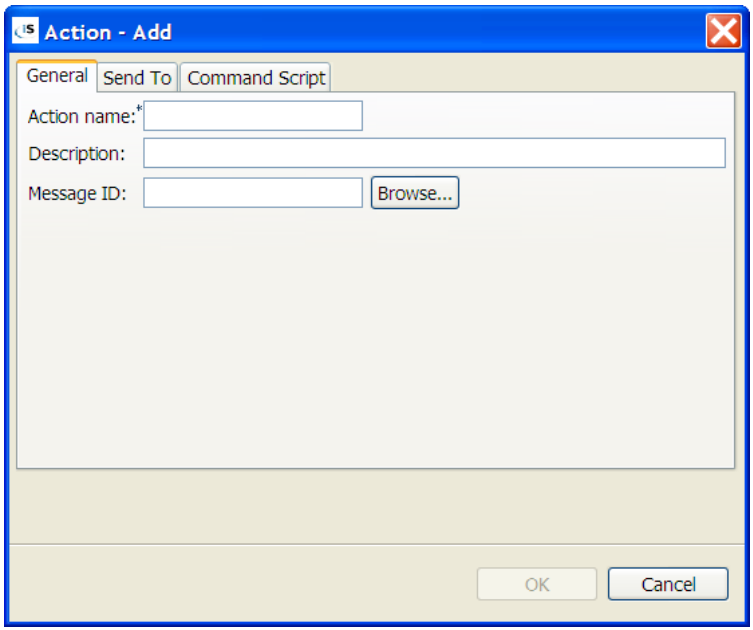
Add Business Alerts

3. Click Browse, the Select Action screen appears



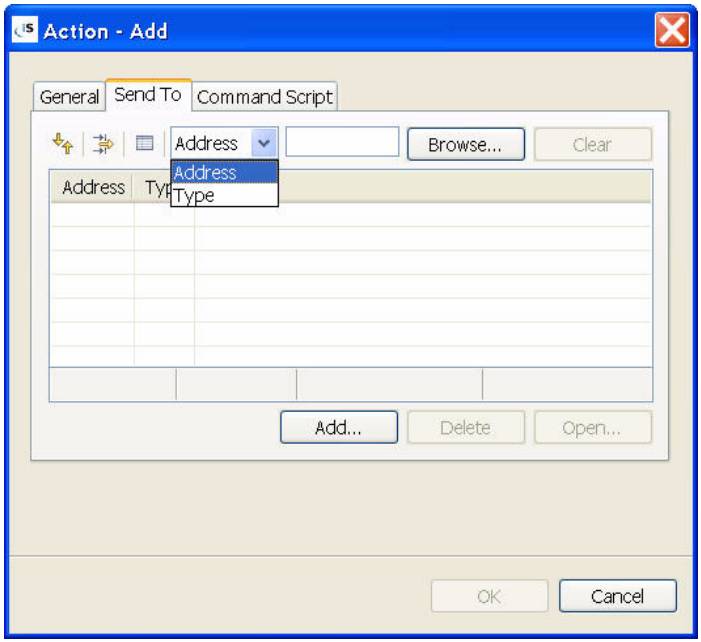
Select Action

4. Click **Add** to add a new action to the list



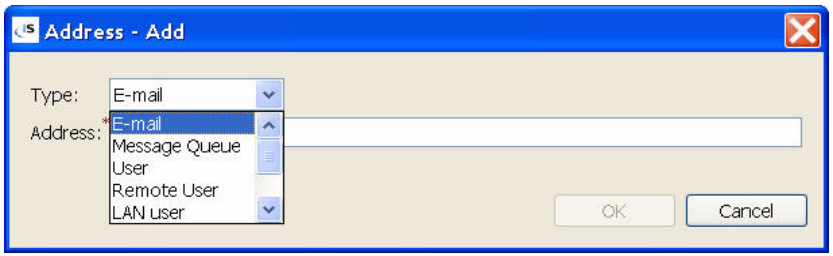
Action - Add

5. Type a name, description and a message ID
6. Select **Send To** tab to set an address for the message to be sent



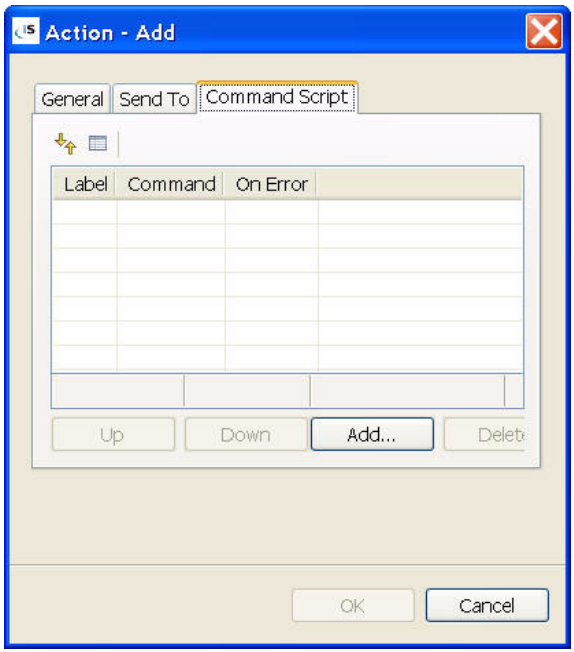
Add Action - Address

7. Click **Add** to add a new address to the list



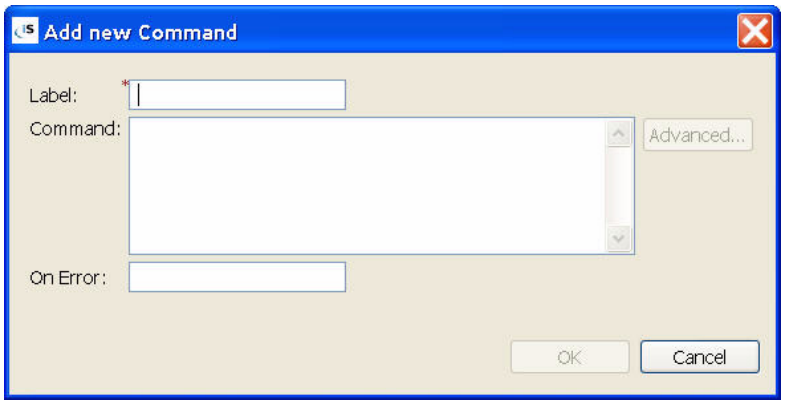
Add Action - Add Address

8. Select **Command Script** tab to add a command for the action



Add Action - Command

9. Click **Add** to add a command to the list



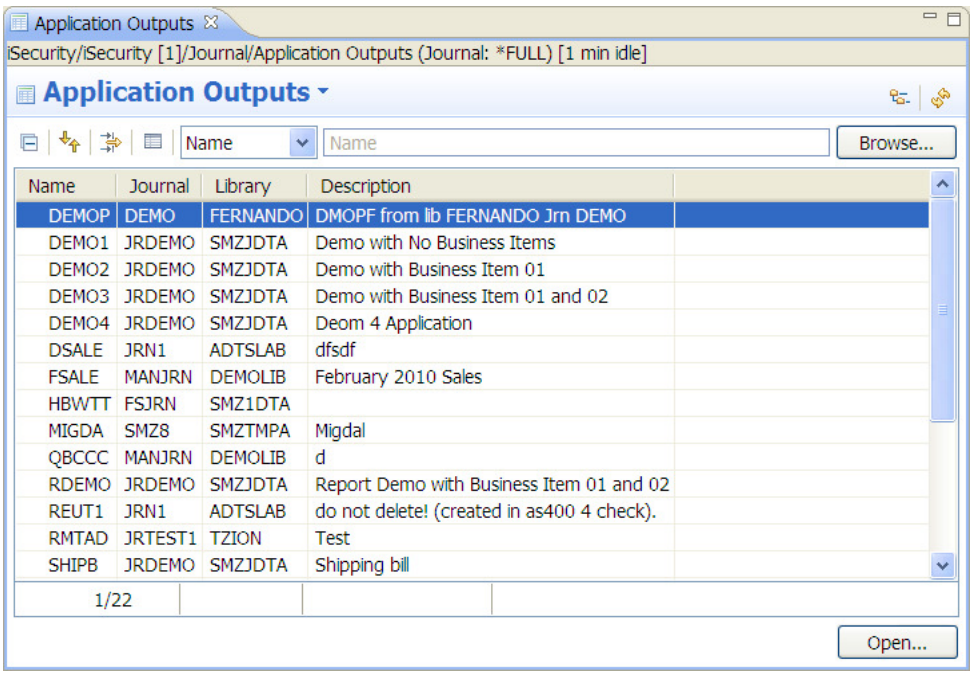
Add Action - Add Command

Edit Actions

1. To edit an action select an action to edit and click **Open**
2. Edit the description, message ID, address and command and click **OK**.

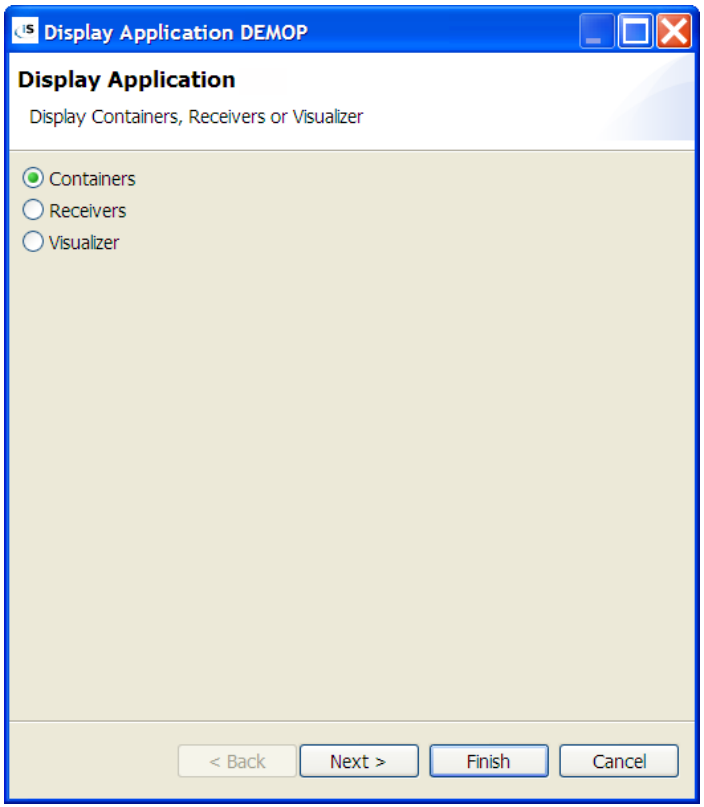
Application Outputs

1. Select **Application Outputs** node to display the application data


Application Outputs
iSecurity/iSecurity [1]/Journal/Application Outputs (Journal: *FULL) [1 min idle]
Application Outputs
Name
Name
Browse...
Name Journal Library Description
DEMOP DEMO FERNANDO DMOPF from lib FERNANDO Jrn DEMO
DEMO1 JRDEMO SMZJDTA Demo with No Business Items
DEMO2 JRDEMO SMZJDTA Demo with Business Item 01
DEMO3 JRDEMO SMZJDTA Demo with Business Item 01 and 02
DEMO4 JRDEMO SMZJDTA Deom 4 Application
DSALE JRN1 ADTSLAB dfsdf
FSALE MANJRN DEMOLIB February 2010 Sales
HBWTT FSJRN SMZ1DTA
MIGDA SMZ8 SMZTMPA Migdal
QBCCC MANJRN DEMOLIB d
RDEMO JRDEMO SMZJDTA Report Demo with Business Item 01 and 02
REUT1 JRN1 ADTSLAB do not delete! (created in as400 4 check).
RMTAD JRTEST1 TZION Test
SHIPB JRDEMO SMZJDTA Shipping bill
1/22
Open...

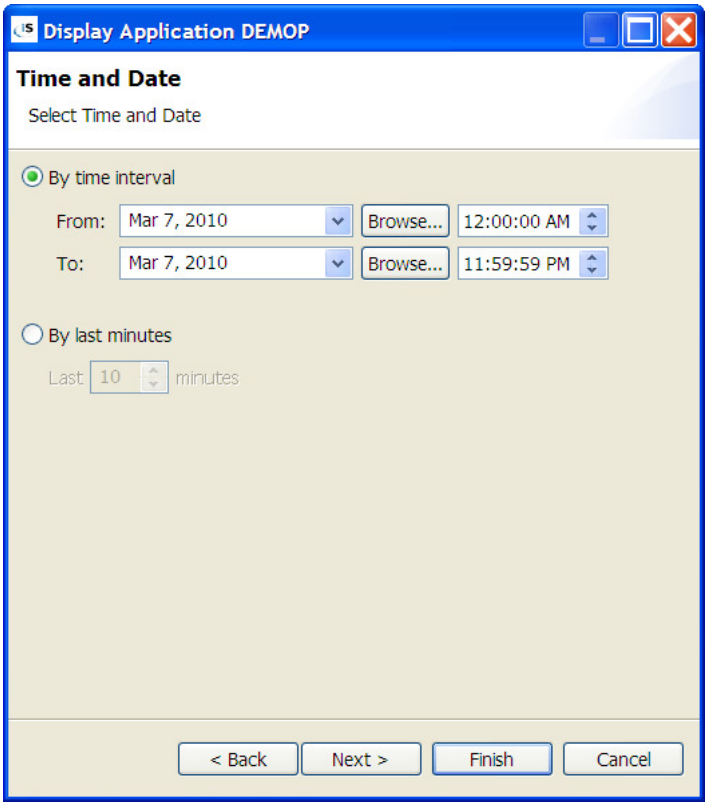
Application Outputs

2. Select application and click **Open**. The **Display Application** screen appears



Display Application

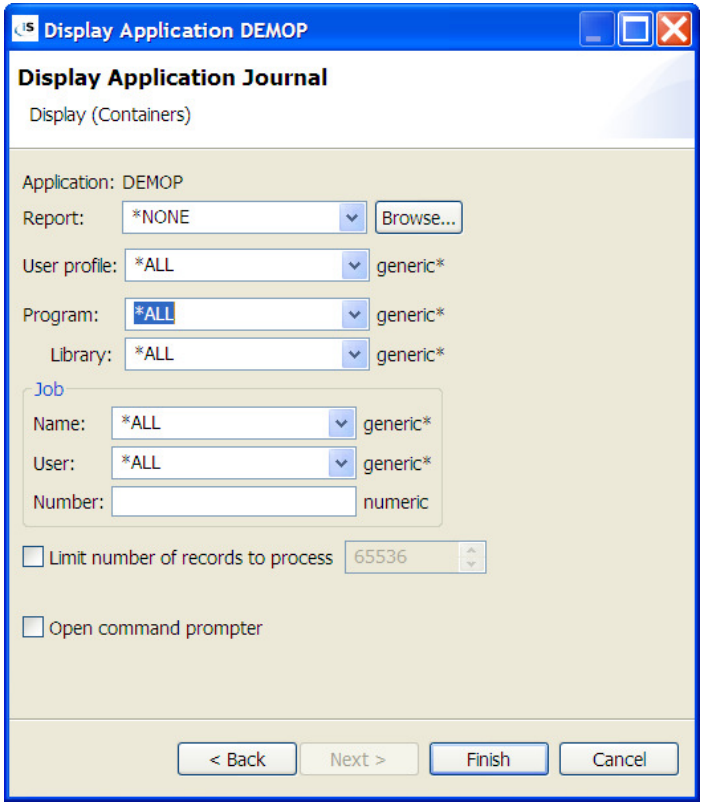
3. Select Container, Receiver or Visualizer and click **Next** to select the time intervals



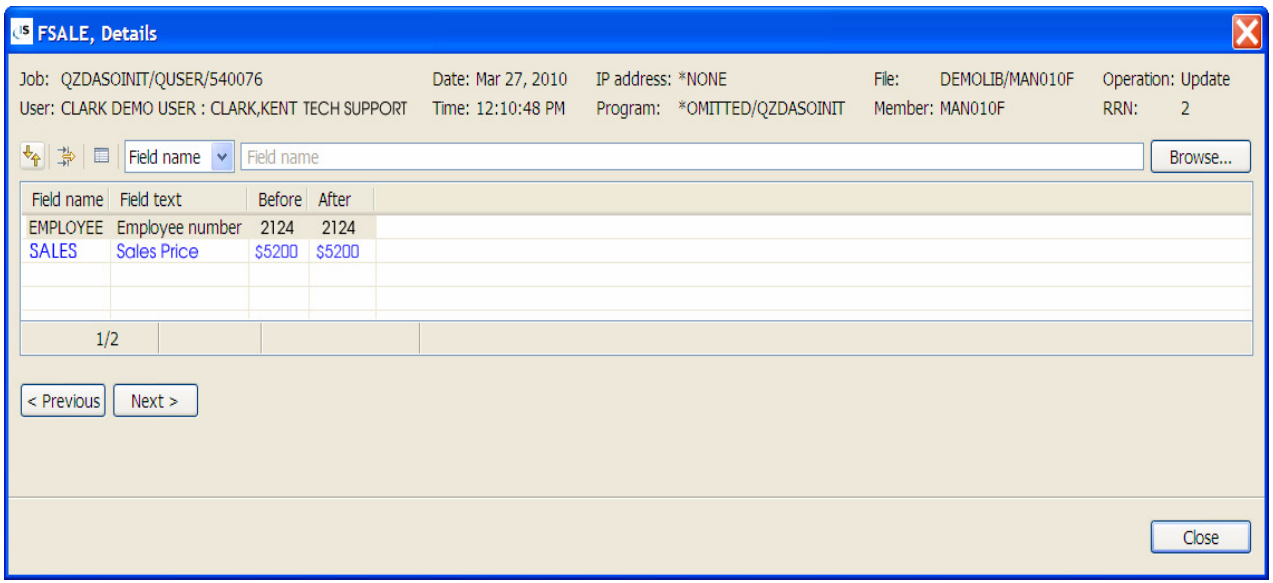
Display Application - Time Interval

4. Select the time intervals and click **Next** to set the report definitions, and click **Finish** to display

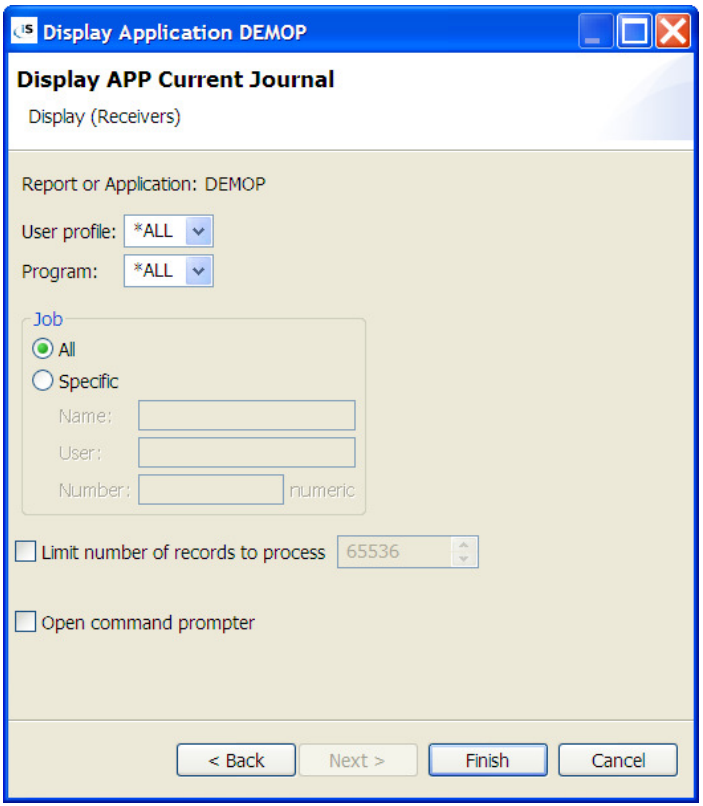
Containers



Display Application - Report Definitions, Container


FSALE, Details
Job: QZDASOINIT/QUSER/540076
Date: Mar 27, 2010
IP address: *NONE
File: DEMOLIB/MAN010F
Operation: Update
User: CLARK DEMO USER : CLARK,KENT TECH SUPPORT
Time: 12:10:48 PM
Program: *OMITTED/QZDASOINIT
Member: MAN010F
RRN: 2
Field name
Field name
Browse...
Field name
Field text
Before
After
EMPLOYEE
Employee number
2124
2124
SALES
Sales Price
$5200
$5200
1/2
< Previous
Next >
Close

Receivers

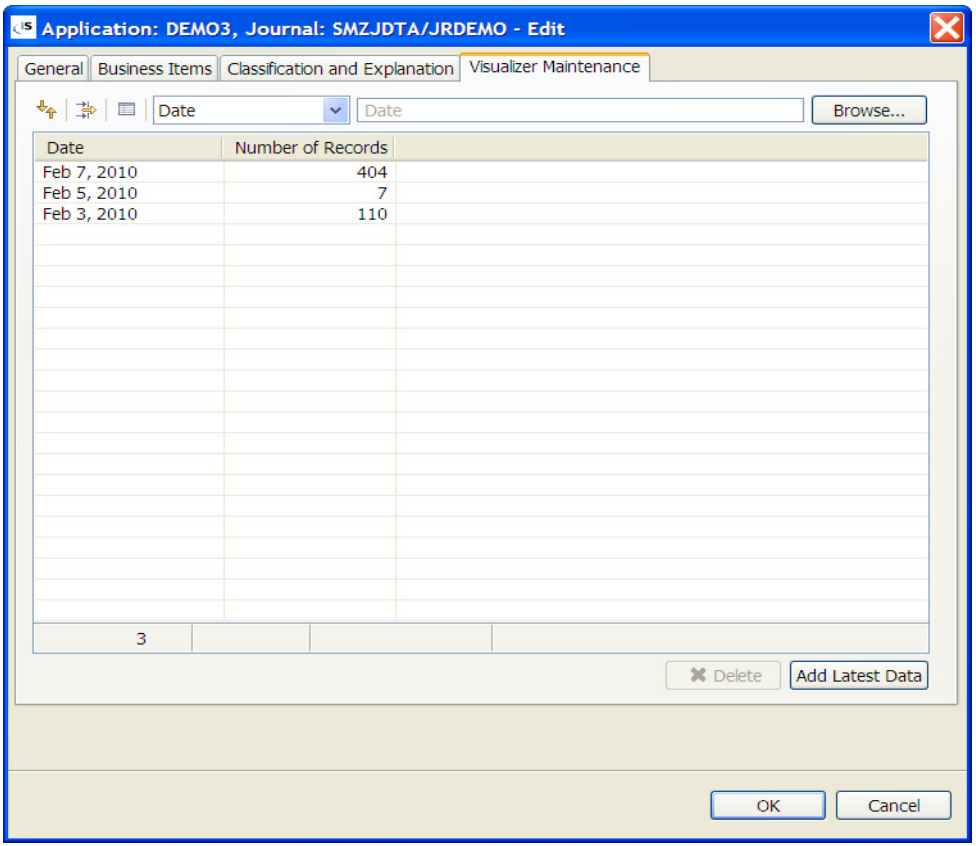


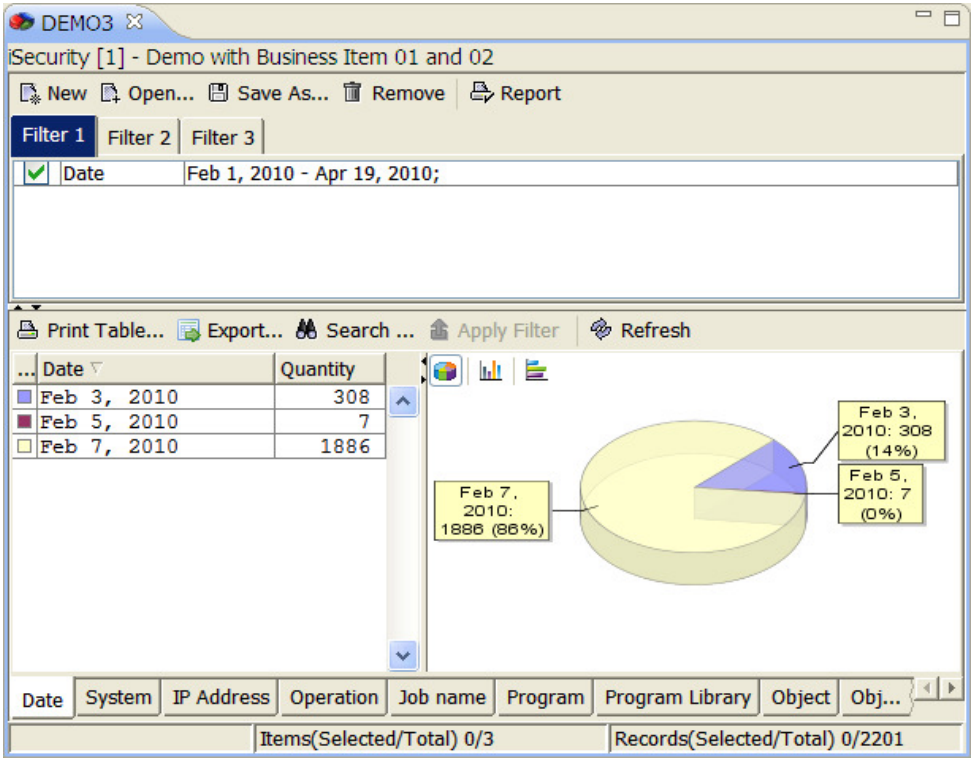
Display Application - Report Definitions, Receivers

Visualizer

Before selecting Visualizer, collect the application data to the application using the Visualizer Maintenance.

1. Select the applicsation form Application Definitions and click Open
2. Select the Visualizer Maintenance tab and click Add Latest Data


Application: DEMO3, Journal: SMZJDTA/JRDEMO - Edit
General
Business Items
Classification and Explanation
Visualizer Maintenance
Date
Date
Browse...
Date
Number of Records
Feb 7, 2010
404
Feb 5, 2010
7
Feb 3, 2010
110
3
Delete
Add Latest Data
OK
Cancel



AP-Journal Visualizer

3

Introducing Business Intelligance - Visualizer

Chapter 3: Introducing Business Intelligence Visualizer

Overview

Business Intelligence - Visualizer is an advanced data warehouse solution that allows IT managers to graphically analyze security-related system activity quickly and easily.

Business Intelligence - Visualizer uses business intelligence techniques to process large quantities of transaction data with minimal storage requirements. This process eliminates the need for time-consuming log scanning and tracking activities that tie up system resources and increase IT operating costs.

With most security analysis products, the system administrator faces a "needle in a haystack" search task in order to analyze security breaches or other critical system activity. **Business Intelligence - Visualizer** makes the whole process painless, simple, and cost-effective.

Business Intelligence - Visualizer presents the user with a user-friendly, JAVA-based GUI, making the whole process a snap, even for technologically-challenged users. The user simply points, clicks, and drags the appropriate parameters to the filter section of the GUI and a stunning pie chart appears in seconds that tells the whole story. Want to tweak the analysis a bit? Simply mouse a few changes and the revised results appear like magic.

Business Intelligence - Visualizer is available in versions that work with **Firewall, Audit** and **AP-Journal**.

Key Features and Benefits

- User-friendly, intuitive GUI
- Lightning fast operation - does not waste precious system resources
- Report generator creates statistical reports with rich graphics
- Works with all significant data elements associated with each transaction type
- Queries may be saved and re-used as necessary
- Available in **Firewall**, **Audit** and **AP-Journal** versions

Installing Business Intelligence - Visualizer

1. Enter the installation CD into your PC and navigate to the **Visualizer** page.
2. Click the installation file and follow any further instructions.
3. Go to **Start/Programs/iSecurity** and enter code.

3

Working with Business Intelligance - Visualizer

Chapter 3: Working with Business Intelligance

Working with Business Intelligence

Business Intelligence is an advanced data warehouse solution that allows IT managers to graphically analyze security related system activity quickly and easily.

Business Intelligence uses a techniques to process large quantities of transaction data with minimal storage requirements. This process eliminates the need for time consuming log scanning and tracking activities that tie up system resources and increase IT operating costs.

With most security-analysis products, the system administrator faces a "needle-in-a-haystack" search task in order to analyze security breaches or other critical system activity. **Business Intelligence** makes the whole process painless, simple, and cost-effective.

Business Intelligence presents a user-friendly interface, making the whole process a snap. Simply point, click, and drag the appropriate parameters to the filter section and a stunning pie chart appears in seconds that tells the whole story. Want to tweak the analysis a bit? Simply mouse a few changes and the revised results appear like magic.

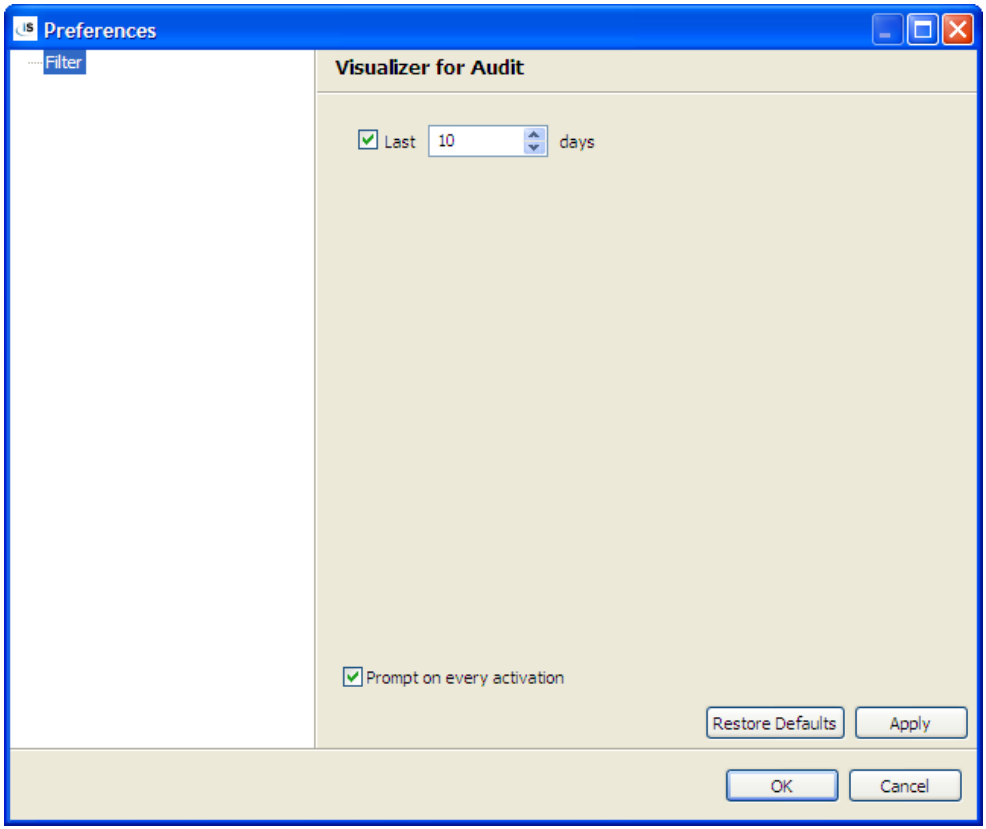
Starting Business Intelligence

The following example is based on Audit Business Intelligance.

To open and begin working with **Business Intelligence**, follow this procedure.

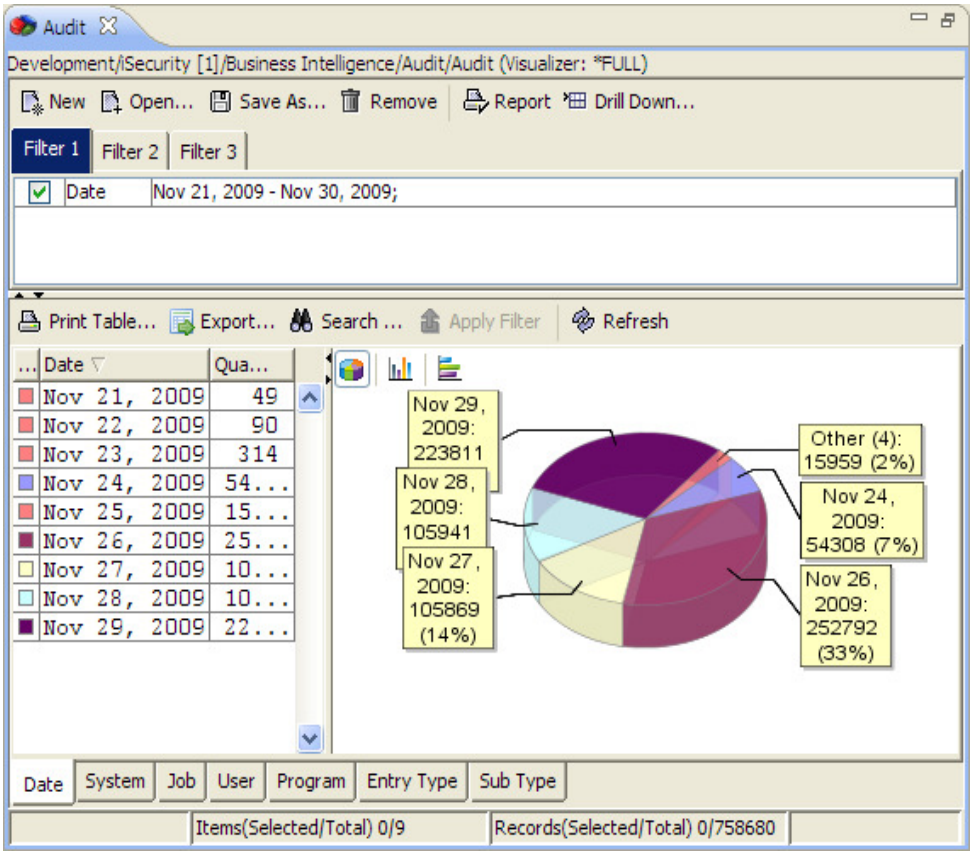
1. Click the **Business Intelligence** node to open the navigation tree.
2. Click **Audit**

> **NOTE:** *In order to work with* **Visualizer** *from* **AP-Journal,** *go to* **Application Outputs** -> *select application* -> *click* **Open** -> *select* **Visualizer**



collect statistical data

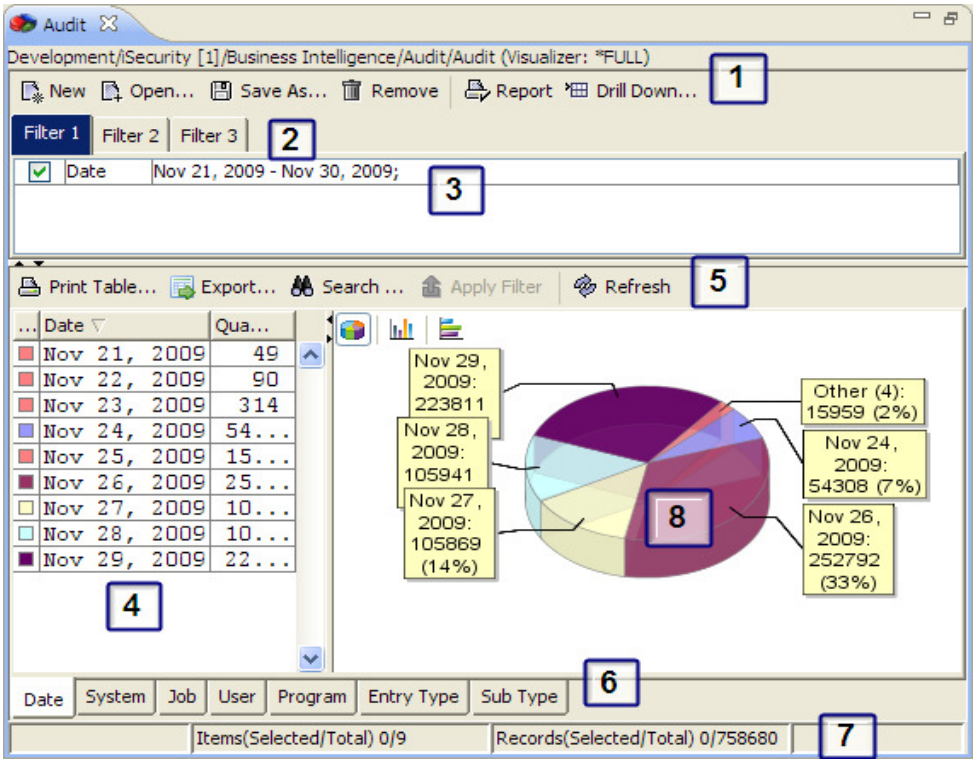
3. Select the number of last days to collect the data from and click OK.
4. Double-click **Firewall** or **Audit** to work with the **Business Intelligence** tool of the product.



Business Intelligance - Audit

The Business Intelligence Interface

The following screen-shot is the main interface window for **Business Intelligence**, the graphic-analysis security component of **iSecurity**. The table below provides a description of the main components.



Business Intelligence (main interface)

Number	Name	Description
1	**Toolbars**	The toolbar enables you to perform basic navigation tasks. **New** = Creates and opens a new filter tab (see *Filter Tabs*) **Open** = Opens a previously-saved filter **Save as** = Enables you to save filter data **Remove** = Delete a filter **Report** = Generates an HTM report **Drill Down**= Filter by specific time and limit number of records to process
2	**Filter Tabs**	Enables you to navigate between open filters

Number	Name	Description
3	**Filter Pane**	Area where filters are displayed
4	**Data Pane Toolbars**	Toolbar that enables you to work with the Data Pane
5	**Data Pane**	Area where Dimension data is displayed. **Print Table** = Print data **Export** = Export data to spreadsheet **Search** = Search and add to the filter **Apply Filter** = Click to apply selection to the filter. **Refresh** = Click **Refresh** after the fetch size has been modified. **Maximum items to retrieve** = the fetch size can be set at any time from within the visualizer. This way you can gradually increase the amount of data being retrieved making it less prone for a long task.
6	**Dimensions**	These criterion enable you to choose how you want to sort and display your data. **Date** = Sorts system activity according to date **System** = Select the system you want to work with **User** = Sorts system activity according to user **Server** = Sorts system activity according to server **Function** = Sorts system activity according to function, such as ***OPEN***, ***DELETE***, etc. **IP** = Sorts system activity according to **IP address** **Library** = Sorts system activity according to library **Object** = Sorts system activity according to object **Result** = Sorts system activity according to Allow or Reject

Number	Name	Description
7	**Status Bar**	The Status Bar, divided into three parts, displays valuable system information. **1.** Number of members (units of information-each displayed on a different line) selected, out of total members. **2.** Number of entries (entries to the system) selected, out of total number of entries. **3.** IP address of computer.
8	**Pie Chart**	The colorful, pie-shaped representation of your security and system data. Display also in a vertical and horizontal bar chat.

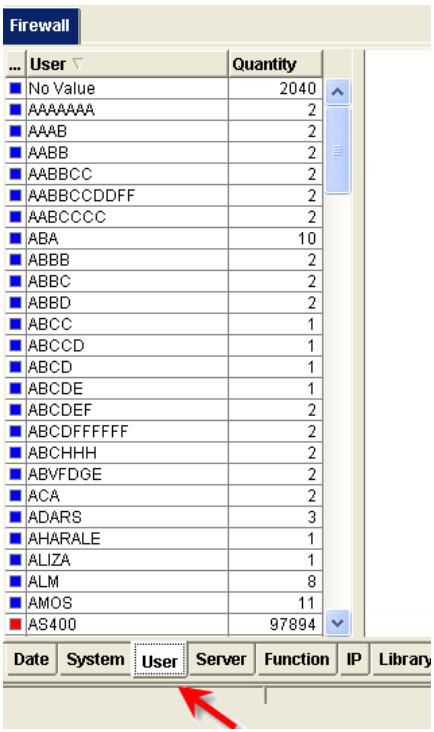
Generating Graphic Reports

NOTE: *Visualizer works with a statistical file installed on your system. Therefore, all dates listed in the* **Date** *dimensions (the default opening setting) in the* **Data** *pane will be from when the first entries were made to your system.*

1. Phrase the data you want to display in this form: (examples). This is known as a **Business Intelligence query.**
   - Date **according to** user (a particular user's entries covering all dates)
   - Server **according to** function (a particular function's entries broken down into a list of the different servers that performed that function)
   - Result **according to** IP (an IP address listed by how many entries were allowed/rejected)
2. Make sure the **Filter** pane is empty, then click the **Dimension** tab of the second part of the **Business Intelligence** query.
3. Find the specific data in the list and select it. Note that the **Filter** pane immediately displays this information.
4. Click the **Dimension** tab of the first part of the **Business Intelligence** query. Your query is displayed in the **Data** pane.

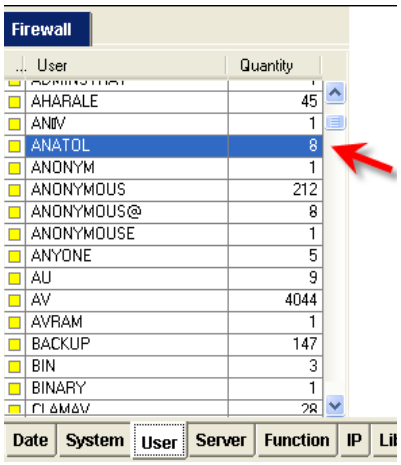
The first example listed, date according to user, is shown this way.

1. Click the **User** Dimension tab.

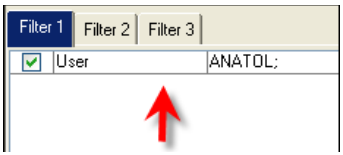


Clicking the User Dimension tab (example)

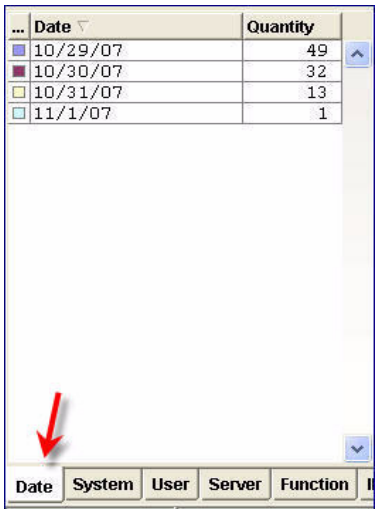
2. Select the user you want to learn about.



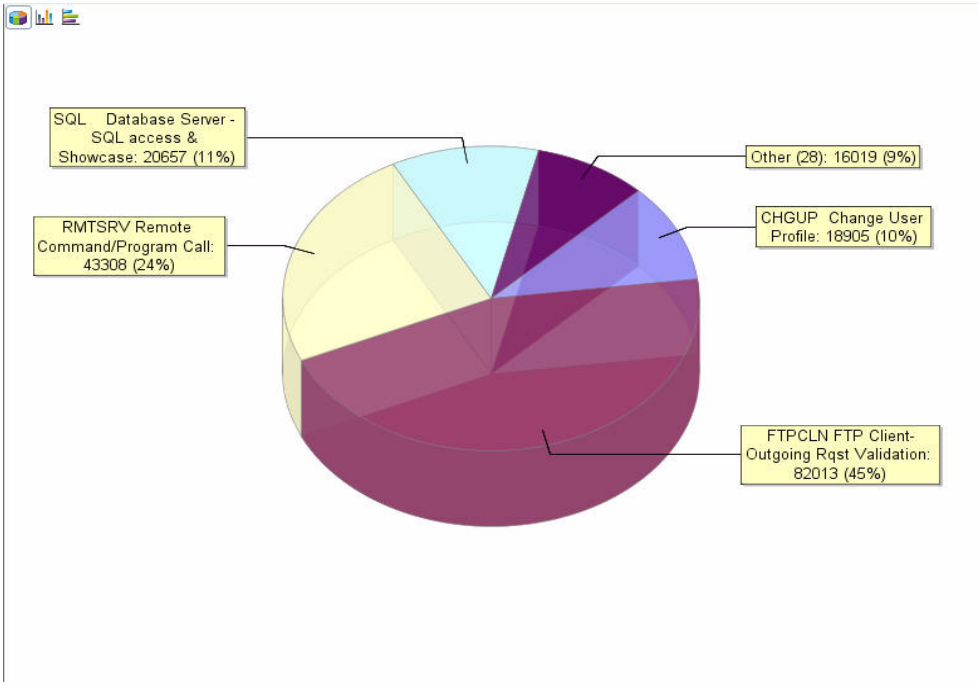
3. Note that this selection is immediately logged in the **Filter** pane.



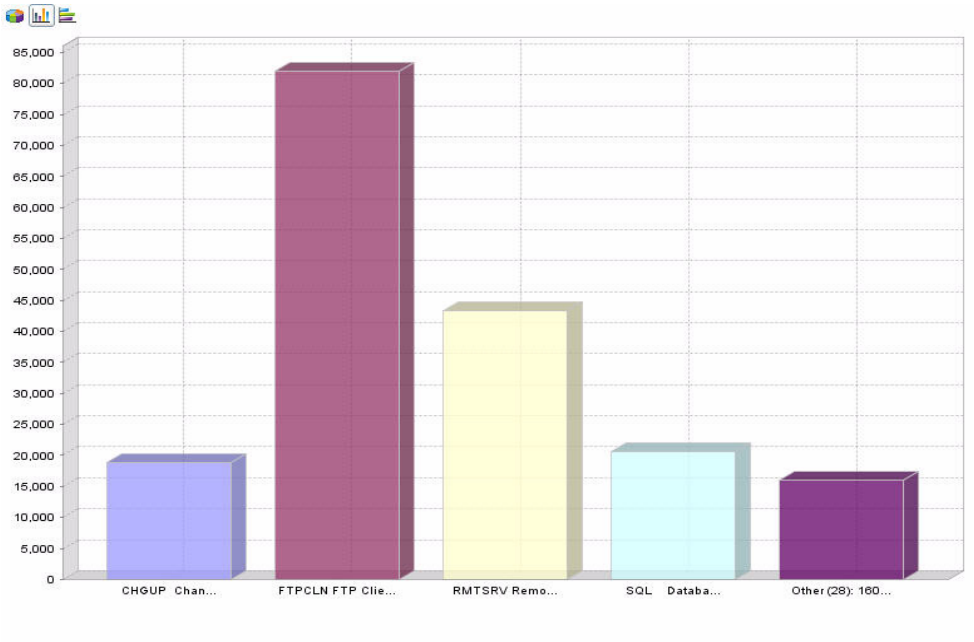
4. Click the tab of the first part of the **Visualizer** query (in this case, **Date**).



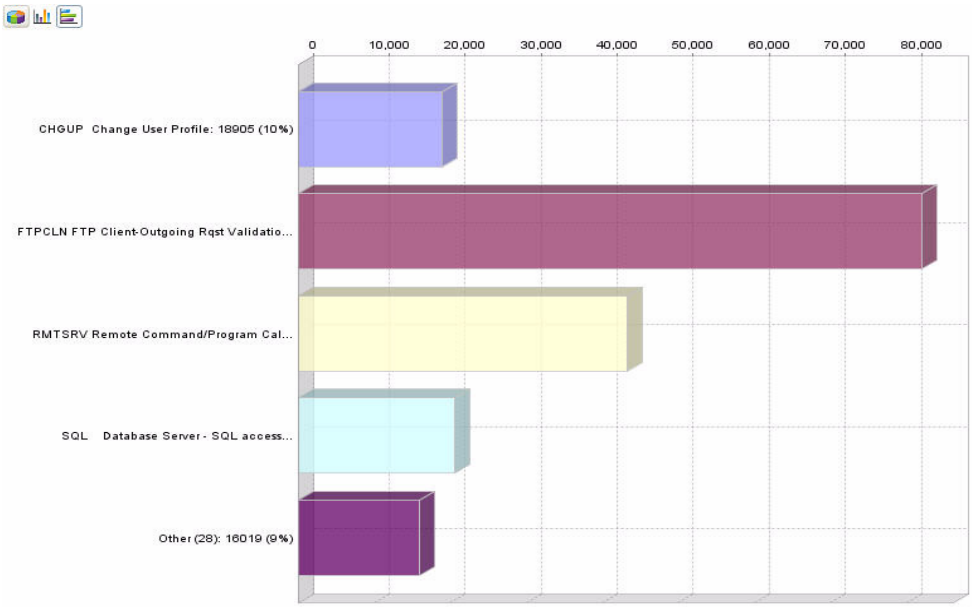
The dates are listed in the **Data** pane immediately or after a few seconds. Next to the date is the number of entries that the user made on each of those dates; the appropriate pie chart is also displayed.


SQL Database Server - SQL access & Showcase: 20657 (11%)
Other (28): 16019 (9%)
CHGUP Change User Profile: 18905 (10%)
RMTSRV Remote Command/Program Call: 43308 (24%)
FTPCLN FTP Client-Outgoing Rqst Validation: 82013 (45%)

Pie Chart



Vertical Bar Chart



Horizontal Bar Chart

Purge history files of Visualizer by SQL

To purge Visualizer history files, use the following SQL Command or any other AS400 file manager such as FileScope:

DELETE FROM SMZTMPA/GSSTTS WHERE STDATE=091023

where

Firewall History file: SMZTMPA/GSSTTS

Audit History file: SMZ4DTA/AUSTTS

License Agreement

Appendix: License Agreement

GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below. When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it. For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library. To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by

obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license. Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library. We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library. The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you". A "library" means a collection of software functions and/or

data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification").

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
    a. The modified work must itself be a software library.
    b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
    c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
    d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied

function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.
4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses

the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessories, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its

terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any

later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promotin g the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. 16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS